| NODIS Library | Legal Policies(2000s) | Search |

NASA
Procedural
Requirements

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

COMPLIANCE IS MANDATORY

Security of Information Technology

Responsible Office: Office of the Chief Information Officer

Table of Contents

Preface

Section I NASA IT Security Program

Chapter 1 Introduction, Laws and Regulations, Capital Planning, and Metrics

Chapter 2 Roles and Responsibilities

Chapter 3 IT Program and System Security Assessments

Chapter 4 Contracts, Grants, and Agreements

Section II Defining The System

Chapter 5 System Development Life Cycle

Chapter 6 Information and Information System IT Security Strategy

Chapter 7 System Characterization, Information Categorization, System Types, and System Boundaries

Chapter 8 Master and Subordinate IT Systems

Chapter 9 System Interconnectivity

Chapter 10 Products and Services

Chapter 11 Security Controls

Section III Management Controls

Chapter 12 IT Security Risk Management

Chapter 13 IT System Security Planning

Chapter 14 System Certification and Accreditation

Chapter 21 Audit Trails and Accountability

Section VI Appendices

Preface

P.1 Purpose

This National Aeronautics and Space Administration (NASA) Procedures and Requirements (NPR) document implements the NASA Policy Directive (NPD) 2810.1, NASA Information Security Program. NPR 2810.1 establishes the procedures and requirements of the NASA Information Technology (IT) Security Program and provides direction designed to ensure that safeguards for the protection of the confidentiality, integrity, and availability of unclassified IT resources are integrated into and support NASA's missions, functional lines of business, and infrastructure based on risk-managed, cost-effective IT security and information security principles and practices.

P.2 Applicability

P.2.1 This NPR applies to all NASA employees, NASA support service contractors, NASA IT resources, and in NASA contracts, grants, purchase orders, and cooperative agreements, where appropriate, in achieving Agency missions, programs, projects, and institutional requirements. Facilities, resources, and personnel under a contract or part of a grant, an international partner agreement, or a volunteer associate's agreement from NASA to a college, university, research establishment, or associate's program are included in the applicability of this document unless specific sections are identified as being waived in the contract, grant, or cooperative agreement.

P.2.2 These procedures and requirements shall be implemented for unclassified NASA information and IT resources that are contracted out or outsourced to (1) another Center; (2) another Government Agency; (3) a Government owned, contractor operated (GOCO) facility; (4) partners under the Space Act; (5) partners under the Commercial Space Act of 1997; or (6) commercial or university facilities. These entities shall be subject to IT security compliance reviews and audits by NASA. Waivers to specific procedures and requirements shall be approved by the cognizant Mission Directorate, Center, or Headquarters Chief Information Officer (CIO) and by the NASA Office of the Chief Information Officer (OCIO).

P.2.3 Any IT resource in or behind the NASA assigned Internet Protocol (IP) address space shall follow NASA and Center policies and requirements and shall be subject to IT security compliance reviews and audits by NASA or its agents. Contractor, grant, international partner's, or research facility's computing and information resources that do not possess NASA information or IT resources, and that are not under direct NASA management cognizance, or are merely incidental to a contract, (e.g., a contractor's payroll and personnel system) are normally excluded from full review or audit to protect proprietary or privacy data.

P.2.4 These procedures and requirements do not apply to Classified National Security Information (CNSI). Specific policy and requirements for CNSI is contained in NPD 1600.2, NASA Security Policy, and NPR 1600.1, NASA Security Program Procedural Requirements.

P.2.5 For purposes of this NPR, NASA Headquarters is treated as a Center. Thus, all roles and responsibilities of the Center CIO are also applicable to the NASA Headquarters CIO. Further, all stipulated Center requirements are also applicable to NASA Headquarters.

P.3 Authority

a. 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended.

b. 5 U.S.C. 552, et seq., the Freedom of Information Act, as implemented by 14 Code of Federal Regulations (CFR) 1206.

c. 5 U.S.C. 552a, the Privacy Act, Pub. L 93-579, as amended.

d. 18 U.S.C. 799, Violation of Regulations of National Aeronautics and Space Administration.

e. 18 U.S.C. 2510, et seq., the Electronic Communications Privacy Act of 1986, as amended.

f. 22 U.S.C. 2751, et seq., the Arms Export Control Act, as implemented by the International Traffic in Arms Regulations, 22 CFR Parts 120-130.

g. 40 U.S.C. 1401, et seq., Chapter 808 of Pub. L 104-208, the Clinger-Cohen Act of 1996 [renaming, in pertinent part, the Information Technology Management Reform Act (ITMRA), Division E of Pub. L 104-106].

h. 42 U.S.C. 201 nt., Health Insurance Portability and Accountability Act of 1996, as amended.

i. 44 U.S.C. 101, E-Government Act of 2002.

j. 44 U.S.C. 3535, Federal Information Security Management Act (FISMA) of 2002.

k. 44 U.S.C. 3501, et seq., Paperwork Reduction Act of 1995, as amended.

l. 50 U.S.C. Appendix 2401-2420, Export Administration Act of 1979, as amended.

m. 14 CFR Part 1206, Availability of Agency Records to Members of the Public.

n. 15 CFR Parts 730-774, Export Administration Regulations.

o. 22 CFR Parts 120-130, International Traffic in Arms Regulations.

p. EO 12958, Classified National Security Information, dated April 17, 1992.

q. EO 13011, Federal Information Technology, dated July 16, 1996.

P.4 References

a. OMB Circular No. A-130, Appendix III Management of Federal Information Resources dated November 28, 2000.

b. OMB Circular A-11, Planning, Budgeting and Acquisition of Capital Assets, dated July 16, 2004.

c. OMB Memorandum M-00-13, Privacy Policies, and Data Collection on Federal Web Sites, dated June 22, 2000.

d. National Telecommunications and Information System Security (NTISS) 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems, dated June 17, 1982.

e. NTISS 100, National Policy on Application of Communications Security to Command Destruct Systems, dated February 17, 1988.

f. Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection, dated December 17, 2003.

g. GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM).

h. NPD 1382.17, NASA Privacy Policy.

i. NPD 1440.6, NASA Records Management.

j. NPR 1441.1, NASA Records and Retention Schedules.

k. NPR 1600.1, NASA Security Program Procedural Requirements.

l. NPD 1600.2, NASA Security Policy.

m. NPR 1620.2, Physical Security Vulnerability Risk Assessments.

n. NPD 2540.1, Personal Use of Government Equipment Including IT

o. NPR 2800.1, Managing Information Technology.

p. NPD 2810.1, NASA Information Security Policy.

q. NPD 2820.1, NASA Software Policy.

r. NPR 2830, NASA Enterprise Architecture.

s. NPR 7100.1, Protection of Human Research Subjects.

t. NPR 7100.8, Protection of Human Research Subjects.

u. NPR 7100.10, Curation of Extraterrestrial Materials.

v. NPR 7120.4, Program/Project Management.

w. NPR 7120.5, NASA Program and Project Management Processes and Requirements.

x. NPR 7120.6, Lessons Learned Process.

y. NPR 7150.2, NASA Software Engineering Requirements.

z. NPR 8000.4, Risk Management Procedural Requirements.

aa. NPR 9900.1, Counterintelligence Procedures and Guidelines.

bb. Federal Information Processing Standards (FIPS). URL: http://csrc.nist.gov/publications/fips/index.html.

cc. National Institute of Standards and Technology (NIST) Special Publications (SPs) 800 Series. URL: http://csrc.nist.gov/publications/nistpubs/index.html.

P.5 Cancellation

a. NPR 2810.1, Security of Information Technology, revalidated August 12, 2004.

b. NITR 2810-1, Wireless Requirements, dated September 15, 2003.

c. NITR 2810-2, Information Technology (IT) System Security Requirements, dated June 28, 2004.

d. NITR 2810-3, NASA Internet Publishing Guidelines, dated December 2, 2004.

e. NITR 2810-4, Information Technology (IT) System Security Certification and Accreditation and Authorizing Systems for Operation, dated December 21, 2004.

f. NITR 2810-5, Information Technology (IT) Security Patch Management System, dated December 14, 2004.

/S/
Patricia Dunnington
Chief Information Officer

DISTRIBUTION: NODIS

SECTION I NASA IT SECURITY PROGRAM

Chapter 1 Introduction, Laws and Regulations, Capital Planning, and Metrics

1.1 Introduction

1.1.1 The overall objective of the Information Technology (IT) Security Program is to provide requirements and direction to ensure that safeguards for IT resources (i.e., data, information, applications, and systems) are integrated into and support NASA's missions and functional lines of business.

1.1.2 Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the Federal Government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

1.1.3 The FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

1.1.4 The security categories of information and IT resources that require protection are as follows:

a. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

b. Integrity. Guarding against unauthorized information modification or destruction, which includes ensuring information non-repudiation and authenticity. Loss of integrity is the unauthorized modification or destruction of information.

c. Availability. Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

1.2 Laws and Regulations

1.2.1 The E-Government Act of 2002, Pub. L. 107-347, recognizes the importance of IT security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the "Federal Information Security Management Act" (FISMA), requires each Federal agency to develop, document, and implement an agencywide IT security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, support service contractor, or source. FISMA directs the National Institute of Standards and Technology (NIST) to publish the appropriate standards and guidance necessary for agencies to implement FISMA.

1.2.2 FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes that a risk-managed policy for cost-effective IT security and information security principles and practices must be addressed throughout the life cycles of the agency's information systems.

1.2.3 NASA's security protections shall be commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the information or information system.

1.2.4 FISMA holds agency heads responsible for ensuring that IT security management processes are integrated with agency strategic and operational planning processes. NASA shall integrate IT security into its capital planning and investment process, its contracting and acquisition strategies, and its program and project life cycle.

1.3 Policy Requirements

1.3.1 NASA IT security polices, requirements, and procedures shall be:

a. Established to implement NIST publications on IT security to support the missions of NASA.

b. Based on the analysis of security risks and the cost-effective reduction of risks to an acceptable level.

c. Apply throughout the life cycle of the information and the information system, and the life cycle processes of programs and projects.

d. Measured and reviewed at least annually to validate effectiveness and to ensure compliance with current Federal policies and guidance.

1.3.2 NASA shall respond to new threats and vulnerabilities, which require policies, procedures, and security controls to be reviewed and modified, on a continuing basis to ensure that information and information systems are adequately protected. To accommodate new threats and vulnerabilities in policy and procedures, NASA shall:

a. Issue NASA Information Technology Requirements (NITRs) documents to keep the NASA IT Security Program current with changes in the IT environment and with changes in Federal policy and guidelines. NASA NITRs shall be incorporated into future revisions of this NPR. Once a NITR has been incorporated into the next revision of the NPR 2810.1, the NITR shall be canceled.

b. Utilize Standard Operating Procedures (SOPs) to ensure consistent implementation and develop educational, technical guidance, and awareness and training materials to ensure a competent, skilled, and up-to-date workforce. Request for deviating from SOPs shall be addressed to the OCIO for approval or disapproval.

c. The OCIO will publish Directive Letters as required to convey short-term requirements such as metrics deliverables.

d. Revisions to NASA security policies, requirements, and procedures (e.g., NITRs and Directive Letters) that affect NASA procurement and non-procurement instruments shall be implemented through action by the contracting officer.

1.4 Capital Planning

1.4.1 Capital Planning Overview

1.4.1.1 FISMA charges agencies with integrating IT security into the Capital Planning and Investment Control (CPIC) processes, which have previously been performed independently by security and capital planning practitioners. NASA must effectively bridge the gap between IT security and capital planning to ensure that available funding is applied toward protecting NASA's IT investments. OMB requires that annual budget packages, submitted under OMB Circular A-11, Exhibits 53 and 300, specifically include the IT security component.

1.4.1.2 FISMA, OMB Circular A-130, Appendix III, and General Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM) security requirements all relate to NIST Special Publication (SP) 800-26, Security Self-Assessment Guide for Information Technology Systems, and the NIST SP 800-53, Recommended Security Controls for Federal Information Systems, because minimum baseline security requirements are discussed.

1.4.1.3 The capital planning requirements contained in FISMA and OMB Circular A-11 impact the capital planning process at Federal agencies. OMB Circular A-11 directs agencies to complete Exhibit 300s and an Exhibit 53.

1.4.1.4 The FISMA report directly impacts the capital planning process. OMB requires that all agencies are in compliance with NIST SP. It is mandatory that the FIPS are followed. As part of this requirement, NASA shall capture all known weaknesses in the Plan of Action and Milestones (POA&M) process. The POA&M is a document that lists the steps necessary to remediate known weaknesses. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. (See Appendix B, Glossary for a definition of the POA&M.) The weaknesses identified are logged into the POA&M. NASA must then determine the costs and timeframes associated with mitigating the vulnerability and correcting security deficiencies. As appropriate, these costs are captured in the Exhibit 300 and rolled into the Exhibit 53, which provides an overview of NASA's IT portfolio. (See Appendix B, Glossary for a high-level definition of Exhibits 300 and 53.) The Exhibit 53 includes a roll up of all Exhibit 300s and additional IT expenses from across NASA. All IT investments are identified by mission area. Investment information includes the budget year and life cycle cost, as well as the percentage of the costs that are devoted to IT security. All costs listed in the Exhibit 300s are totaled across NASA to provide an overall picture of the NASA's IT portfolio.

1.4.2 Capital Planning Requirements

1.4.2.1 NASA shall follow NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Program, for guidance on capital planning.

1.4.2.2 NASA capital planning and investment strategies, at all levels, shall, as a minimum:

a. Identify the IT security requirements necessary for certification and accreditation (C&A) of all IT investments and ensure that resources are available.

b. Provide the resources necessary to implement and operate IT security requirements throughout the life cycle of the IT investment.

c. Track IT security requirements, as a critical element, in the CPIC process and all program management reviews.

d. Require the identification and approval of funding necessary to remediate weaknesses identified in NASA system's POA&M as dictated by the most recent OMB requirements.

e. Require that IT security funding is integrated into NASA's Exhibit 300s and Exhibit 53s and that the exhibits are cross-referenced to NASA's Reporting Repository and Development Database (R2D2).

1.4.2.3 All NASA program reviews, including Independent Assessments (IA), Non-Advocate Reviews (NAR), and the program and project plans shall include the following critical elements:

a. Identify the information category, potential impact, and the Federal Laws restricting distribution of the information that is expected to be processed, stored, or handled throughout the life cycle of the program or project.

b. Identify the IT security requirements necessary for certification and accreditation of all IT investments.

c. Identify the resources necessary to implement IT security requirements throughout the life cycle of the IT investment.

d. Track IT security requirements until mitigated as a critical risk element.

1.4.2.4 NASA Space Act Agreements shall address capital planning, if appropriate, to include:

a. Identifying the information category and potential impacts.

b. Identifying the Federal Laws restricting distribution of the information that will be processed, stored, or handled.

c. Specifically assigning IT security roles and responsibilities to the Space Act Agreement parties.

d. Identifying and documenting the approval authority necessary to grant exceptions to Federal Laws and NASA policies and requirements.

e. Providing for the reporting and investigation of IT security incidents and non-compliance with Federal Laws and NASA policies.

f. Identifying the IT security requirements necessary for C&A of all IT investments.

g. Providing the necessary resources for implementing IT security requirements throughout the life cycle of an IT investment.

1.5 Metrics

1.5.1 The obligation to measure performance and reduce cost is driven by Federal regulatory and NASA requirements. These measurements shall be based upon NASA's goals and objectives, be designed to provide substantive justification for decision-making, and be utilized to measure the effectiveness of the IT Security Program, policies, and requirements. IT Security Program measurement goals and objectives are not static and will be adjusted as the operating environment, threats, and requirements evolve.

1.5.2 Metrics Requirements

1.5.2.1 NASA IT security metrics will be presented to Center Directors and Associate Administrators and will be used to assess the performance of Centers and Agency installations.

1.5.2.2 NASA IT security metrics shall be established by the OCIO Directive Letters.

1.5.2.3 NASA IT security metrics shall address specific IT security controls, assessment findings, or audit findings.

1.5.2.4 NASA IT security metrics shall be analyzed and evaluated by the OCIO, at least annually, for effectiveness in risk reduction and for cost versus impact on return on investment.

1.5.3 Additional IT Security Program References.

a. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

b. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

c. NIST SP 800-55, Security Metrics Guide for IT Systems.

d. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.

e. NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Program.

Chapter 2 Roles and Responsibilities

2.1 Roles and Responsibilities Overview

2.1.1 To implement the various Federal and NASA policies and requirements, FISMA allows for the delegation of IT Security Program responsibilities to various functional roles. NASA senior managers establish the Agency's IT Security Program and its overall program goals, objectives, and priorities. The NASA IT Security Program involves all staff in some capacity. NASA Headquarters, Centers, and support service contractor sites have the latitude to use their internal organizational structure to fulfill the roles and responsibilities described in this chapter if the approach is documented in policy or guidance. The following roles and responsibilities identify key personnel in the IT Security Program.

2.1.2 NIST provides detailed information on IT security-related roles and responsibilities. These are found throughout each NIST document addressing specific IT security elements.

2.2 Senior Management

2.2.1 Senior IT Security Management

2.2.1.1 Ultimately, responsibility for the success of the NASA IT Security Program lies with its senior managers. They establish NASA's IT Security Program and its overall goals, objectives, and priorities to support NASA's mission. NASA managers may delegate to others the responsibility of ensuring that IT security controls, requirements, and procedures are implemented, measured, and improved via life cycle processes.

2.2.1.2 High-level roles and major responsibilities are addressed in this section. They establish the basis for the employee's awareness and compliance by following all applicable security practices and expecting the same of others. See Figure 2-1.

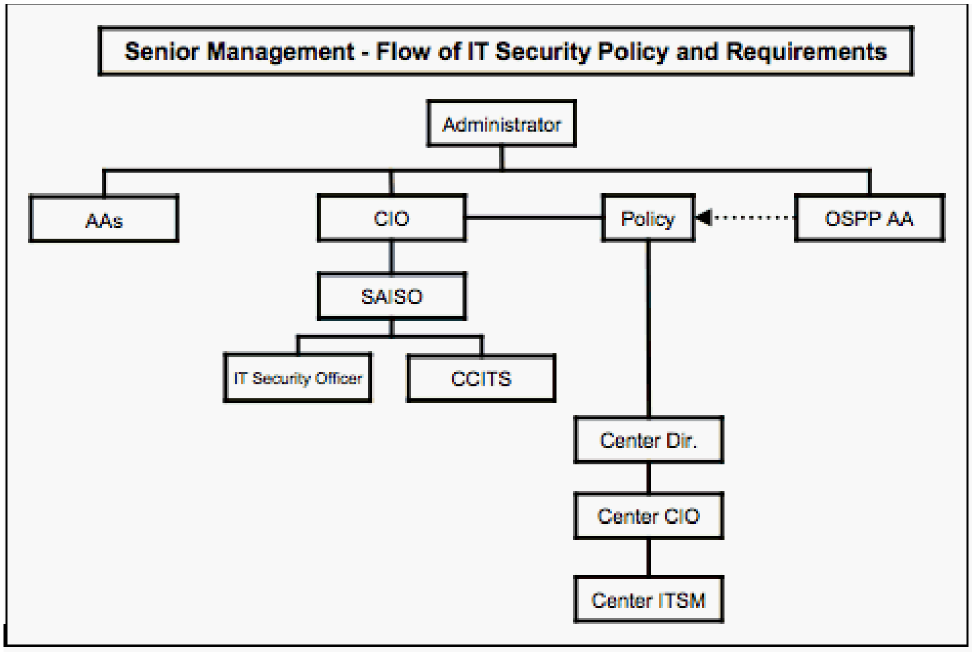


Figure 2-1 NASA Senior IT Security Management Working Relationship

2.2.2 NASA Administrator

2.2.2.1 In accordance with FISMA, the NASA Administrator is responsible for:

a. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use disclosure, disruption, modification, or destruction of 1) information collected or maintained by or on behalf of NASA, and 2) information systems used or operated by NASA or by a contractor of NASA.

b. Agency compliance with Section 11331 or Title 40 U.S.C., including related policies, procedures, standards, and guidelines.

c. Agency compliance with information security standards and guidelines for national security systems issued in accordance with law and as directed by the President.

d. Ensuring that information security management processes are integrated with strategic and operational planning processes.

e. Ensuring that senior Agency officials provide information security for the information and information systems that support the operations and assets under their control.

2.2.2.2 To ensure compliance with the responsibilities of 2.2.2.1, the following delegations are effected by the Administrator:

a. The NASA CIO is delegated the authority to coordinate with the NASA Mission Directorate Associate Administrators, Heads of Mission Support Offices, Center Directors, and NASA program managers to reallocate funds as required to ensure compliance with IT security requirements.

b. The Head of the Office of Security and Program Protection (OSPP) is delegated the responsibility for protecting classified national security information.

c. The Agency Principal Accreditation Authority (PAA), as appointed by the NASA Administrator, is delegated responsibility for establishing and implementing a standardized approach for the certification and accreditation of NASA's National Security Systems (NSS), which includes collateral, sensitive compartmented information (SCI), and special access programs (SAP). The PAA shall ensure the implementation of National Security Telecommunications and Information System Security Instruction (STISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP) and duly appoint a Designated Approval Authority (DAA) process for collateral national security systems, as well as appropriate certification and accreditation processes for SCI and SAP national security systems.

2.2.3 NASA CIO

2.2.3.1 The NASA CIO shall maintain an effective and economical information resource management (IRM) program and ensure that standards and policies for using IT resources incorporate effective protection measures. A key element of the IRM program is protecting information resources. To this end, the NASA CIO is responsible for IT security and has the management oversight responsibilities for ensuring the confidentiality, integrity, and availability of IT resources.

2.2.3.2 The NASA CIO shall establish policies and requirements necessary to comply with FISMA and ensure that NASA information and information systems are protected.

2.2.3.3 To accommodate new threats and vulnerabilities, the NASA CIO shall issue NITR documents to keep current with changes in the IT environment and with changes in Federal guidelines.

2.2.3.4 The NASA CIO shall issue directives, as necessary, to measure the effectiveness of IT security activities, collected data, and analyzed information for trends and to report to NASA management and OMB on the status of the NASA IT Security Program.

2.2.3.5 The NASA CIO shall work with the Mission Directorates, Support Offices, Centers, and program managers to reallocate funds to ensure that NASA complies with FISMA and OMB directives.

2.2.3.6 To implement the NASA-wide IT Security Program effectively, the NASA CIO shall:

a. Appoint a Deputy CIO for IT Security to fill the FISMA role of Senior Agency Information Security Officer (SAISO) and to establish and implement the NASA-wide IT Security Program.

b. Delegate to the OSPP the responsibility for establishing and managing the certification of IT Systems advocate.

c. Establish the NASA Enterprise Architecture to integrate IT security into the strategic planning, capital planning and investment processes.

d. Establish a Competency Center for IT Security (CCITS) to advise and support the SAISO, NASA Authorizing Officials (AOs), Mission Directorate CIOs, Center CIOs, and Center IT Security Managers (ITSMs).

e. Establish a CIO Board to review Agencywide systems to ensure a consistent implementation of security requirements.

f. Provide IT security advice and support to the CPIC processes.

2.2.4 NASA Deputy CIO for IT Security/Senior Agency Information Security Officer

2.2.4.1 The Deputy CIO for IT Security serves as the SAISO. The SAISO is responsible for implementing the IT Security Program of NASA and providing advice and assistance to the Administrator, the NASA CIO, and other senior Agency personnel with IT security roles and responsibilities. The SAISO interacts with external groups regarding IT security, including OMB, Congress, and other Federal agencies and entities exhibiting IT security best practices and plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks.

2.2.4.2 The SAISO shall manage, coordinate, and maintain the overall direction and structure of the NASA IT Security Program.

2.2.4.3 The SAISO shall establish SOPs to provide implementation guidance to ensure consistency of IT security objectives and solutions.

2.2.4.4 The SAISO shall recommend NITRs as interim policy and requirements necessary to address new issues and to clarify existing policy and requirements.

2.2.4.5 The SAISO shall:

a. Appoint an IT Security Officer to oversee and direct NASA-wide IT Security Services such as the IT Security Awareness and Training Center, the NASA Incident Response Center (NASIRC), and the NASA Security Operation Center (NSOC).

b. Oversee, direct, and approve the activities of the CCITS by establishing a Cost, Schedule, and Performance Agreement (CSPA).

c. Charter, oversee, and chair a Network Security Control Board (NSCB) to focus on changes that affect the IT security of NASA at the demarcation of the Agency's Wide Area Network (WAN) and external connectivity. The NSCB will also address IT security network changes within that affect multiple centers. The SAISO shall approve the membership on the NSCB. The SAISO can delegate the role of NSCB Chair.

d. Establish expert centers and ad hoc working groups, as necessary, to assist in developing and implementing the NASA IT Security Program.

e. Provide advice and assistance to the Administrator, NASA CIO, program managers, and other senior Agency personnel to ensure that Agency IT security goals, priorities, and requirements are effectively addressed to protect NASA's investment in IT resources.

f. Recommend metrics to the NASA CIO to measure the IT security posture of NASA to comply with Federal requirements.

2.2.4.6 The SAISO shall review the CPIC processes to ensure that:

a. NASA's Exhibit 300s and Exhibit 53s submitted to OMB identify and adequately provide for implementing IT security requirements.

b. Master and subordinate IT systems map to investments as defined by OMB Exhibit 53 or Exhibit 300.

2.2.4.7 The SAISO shall coordinate with the OSPP to ensure that the IT security assessment and certification activities are adequately supporting the NASA CIO in complying with FISMA and OMB requirements.

2.2.4.8 The SAISO shall track progress of all master and subordinate IT system POA&M items whose scheduled completion date may impact NASA's compliance with FISMA and OMB requirements and report to the NASA CIO in time for corrective action to be taken.

2.2.4.9 The SAISO shall provide a mechanism to ensure that all IT resources comply with standard operating system benchmark templates. NASA will evaluate each system's operating system through a vendor-provided benchmarking capability.

2.2.4.10 The SAISO shall work closely with the Office of Procurement in the development of Agencywide IT security clauses and provisions for incorporation into requests for proposals, requests for quote and statement of work, and other solicitations and procurement and non-procurement instruments.

2.2.5 Office of Security and Program Protection

2.2.5.1 The OSPP is responsible for all aspects of classified national security information matters, including establishing the certification and accreditation policies, procedures, and guidance for all classified IT systems operations. The OSPP responsibilities also include providing the OCIO with support in assessing and certifying unclassified IT systems and ensuring compliance with FISMA and Federal requirements.

2.2.5.2 The Assistant Administrator for OSPP shall:

a. Establish personnel screening policies and requirements for access to IT resources.

b. Ensure that the NASA Counter Intelligence (CI) Program coordinates with the Center ITSMs on matters regarding threats to NASA IT systems and network infrastructure.

c. Coordinate with the SAISO, the CCITS Manager, and NASIRC in the issuance of IT security alerts regarding potential threats and exploits that could affect NASA IT resources and network infrastructure.

d. Support the C&A process and assessments of unclassified IT systems with personnel security and physical security experts and advice.

e. Cooperate with the NASA Office of Inspector General (OIG) on law enforcement matters dealing with cyber counterintelligence (CI) and cyber espionage investigations in accordance with NPR 1600.1, NASA Security Program Procedural Requirements.

f. Appoint an Information Assurance Officer (IAO) to implement an information assurance program to:

(1) Provide internal assessments of IT security policy compliance.

(2) Establish a certification program for systems with an IT security category of moderate or high, in compliance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

(3) Issue requirements for the protection, handling, and destruction of administratively controlled information (ACI) or sensitive but unclassified (SBU) information.

2.2.5.3 The Deputy Assistant Administrator for OSPP is assigned the role of AO for OSPP's master systems and shall:

a. Make the security accreditation decisions for OSPP master systems, which establish the IT security posture of the master and their subordinate systems.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA Chief Financial Officer (CFO) and CIO that funding be redirected to implement security controls required for master or subordinate systems to achieve full Authorization to Process (ATO).

d. Concur or non-concur on the determination of master system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls which will be inherited by any subordinate system under the authority of the master system.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.2.6 NASA IT Security Officer (ITSO)

2.2.6.1 The ITSO shall ensure the effectiveness of:

a. NASA IT security projects crossing Centers.

b. The collecting, analyzing, and reporting of metrics established by the OCIO.

c. The NASA IT Security Awareness and Training Program.

d. NASIRC.

e. The NASA WAN services.

2.2.6.2 The ITSO shall oversee, direct, and approve the activities of the SAISO established NASA IT Security Projects via establishing CSPAs.

2.2.6.3 The ITSO shall recommend metrics to the SAISO to measure the IT security posture of NASA to comply with Federal requirements.

2.2.7 Manager, Competency Center for IT Security

2.2.7.1 The Competency Center for IT Security (CCITS) is the NASA CIO's authorized organization to perform Agencywide IT security leadership, develop and oversee IT security initiatives program management, and perform technology investigation to ensure NASA's pre-eminence in securing its information technology resources with minimal risk and highest efficiency.

2.2.7.2 The CCITS Manager shall:

a. Annually develop a CCITS CSPA that is responsive to the NASA and CIO priorities and directions.

b. Report to the NASA SAISO and be accountable for project schedule, budget, and deliverables, and understand and adhere to the above operating structure of the CSPA.

c. Communicate regularly with the NASA SAISO to ensure that the IT security recommendations, goals, schedules, and budgets are current and on track.

d. Report on progress against the CSPA at least quarterly.

e. Involve NASA Mission Directorate, Centers, and other stakeholders to ensure the timely introduction of new or revised standards or new services with the goal of implementing technically superior solutions, cost effectiveness, and minimal disruption or negative impact upon the IT operational infrastructure and programs of NASA.

f. Continually engage constituencies from other NASA Centers and other Agencies in the definition and implementation of architectures, standards, guidelines, and services.

2.2.8 Center Directors and the Assistant Administrator for Infrastructure and Administration

2.2.8.1 Center Directors and the Assistant Administrator for Infrastructure and Administration are responsible for protecting the Center's missions and programs, advocating support for IT security requirements, and providing the resources necessary to implement the IT security requirements.

2.2.8.2 The Center Directors and the Assistant Administrator for Infrastructure and Administration shall:

a. Delegate the responsibility for the Center IT security program to the Center CIO.

b. Provide adequate funding to programs/projects to implement the Center IT security program and to be compliant with FISMA and NASA requirements.

c. Appoint an ITSM to assist the Center CIO by providing organization and direction for implementing the NASA IT security program.

d. Ensure that IT capital planning and investments address and fund IT security requirements.

e. Ensure that employees and support service contractors are held accountable for adhering to IT security policies and requirements.

f. Ensure IT investments comply with the NASA Enterprise Architecture.

g. Ensure the Center Privacy Act Manager works with the Center ITSM and IAO to protect information subject to the Privacy Act.

2.2.9 Center Chief Information Officer

2.2.9.1 The Center CIO is responsible for establishing an effective and economical Center Information Resource Management (IRM) program. The IRM program plan defines the design and operation of the Center's information infrastructure (e.g., networks, servers, and electronic forms) and ensures alignment with the NASA IRM's vision, mission, and strategy. The Center IT security roles and responsibilities shall reside within the Center CIO office.

2.2.9.2 The Center CIO shall:

a. Establish and chair the Center Network Configuration Control Board (NCCB) to conduct a risk assessment for modifications to the network, to approve or disapprove all modifications, and to provide notification to its customers of all modifications that would affect the protections provided by the network. The Center CIO may delegate the NCCB chair function.

b. Ensure that civil service Organization Computer Security Officials (OCSOs) have the appropriate knowledge, skills, and abilities and are assigned to facilitate the implementation and oversight of the IT security of systems within their organization. For non-NASA facilities or organizations, a non-civil servant may serve as an OCSO.

c. Provide the Center ITSM with sufficient resources to ensure Center compliance with IT security requirements.

d. Manage the Center's network infrastructure to protect information system owners and to control unauthorized internet protocol (IP) addresses.

e. Establish an IT security incident response capability that is accountable to the Center ITSM.

f. Designate a Center-wide certification agent (CA) who shall:

(1) Oversee and assist information system owners in the self-assessments process required for

certification.

(2) Assist information system owners in determining information security categories for systems.

(3) Assist information system owners in determining the appropriate system boundaries and security controls.

(4) Ensure that the activities and documentation required in the initiation phase of the C&A process are completed.

g. Delegate to the Center ITSM the authority to determine when an IT security incident is placing NASA's missions, its customers, its reputation, or its assets in immediate jeopardy to a degree that the Center must exercise its responsibility to unilaterally control or terminate incidents. Actions should be coordinated prior to being implemented with the Center CIO, Center Chief of Security (CCS), the OIG, impacted information system owners, and Information System Security Officials (ISSOs), as soon as practicable.

2.2.9.3 The Center CIO is assigned the role of the AO for the following IT systems.

a. Office Automation of Information Technology (OAIT) subordinate systems;

b. OSPP subordinate systems.

c. Multi-Program subordinate systems (i.e., systems supporting multiple Mission Directorates who share the operating cost, but where no Mission Directorate funds a majority portion of the operational cost).

2.2.9.4 The Center CIO, as an AO, shall:

a. Make the security accreditation decisions for the relevant master systems, which establish the IT security posture of the master and their subordinate systems.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA CFO and CIO that funding be redirected to implement security controls required for the subordinate systems to achieve full authorization to operate (ATO).

d. Concur or non-concur on the system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls inherited from the master system. Non-concurrences shall indicate that the system needs to be aligned with a different master or that a new master system must be created.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.2.10 Center IT Security Manager

2.2.10.1 The Center ITSM is responsible for implementing the Center IT Security Program. The Center ITSM's role is to develop Center-wide IT security policies and guidance, to coordinate and facilitate IT security awareness and training, to maintain an incident response capability, and to document, review, and report the status of the Center IT Security Program.

2.2.10.2 The Center ITSM shall:

a. Support the Center CIO to ensure compliance with NASA policies, requirements, and directives from the OCIO.

b. Develop Center-wide IT security policies and guidance for approval by the Center CIO.

c. Assist Center organizations on all aspects of IT security throughout the life cycle of their IT systems.

d. Conduct periodic assessments and compliance checks.

e. Maintain and track the status of all system security plans (SSPs) assigned to their Center for compliance with NIST and guidance from the NASA SAISO.

f. Track and report the Center's POA&M and IT security metrics status to Center and Agency management.

g. Implement Center vulnerability scanning, patch management, operating system configuration, and penetration testing program to ensure that controls are in place and effective.

h. Develop an incident response capability in coordination with the CCS and the OIG, following the guidance provided by the SAISO for handling and reporting incidents.

i. Coordinate and facilitate the Center IT security awareness and training program.

j. Be an advisor to the chair of the Center NCCB and a member of the Center's NCCB.

k. Have the authority to disconnect or deny service to any network attached device, including wireless, in the event of an incident or violation of acceptable use policy.

l. Provide the Procurement Office with IT security requirements to support preparation of solicitation documents.

2.3 IT Security System and Information Owners

2.3.1 Many individuals at both the Agency and Center levels have key roles to oversee the implementation of a sound IT Security Program within their areas of responsibility. See Figure 2-2.

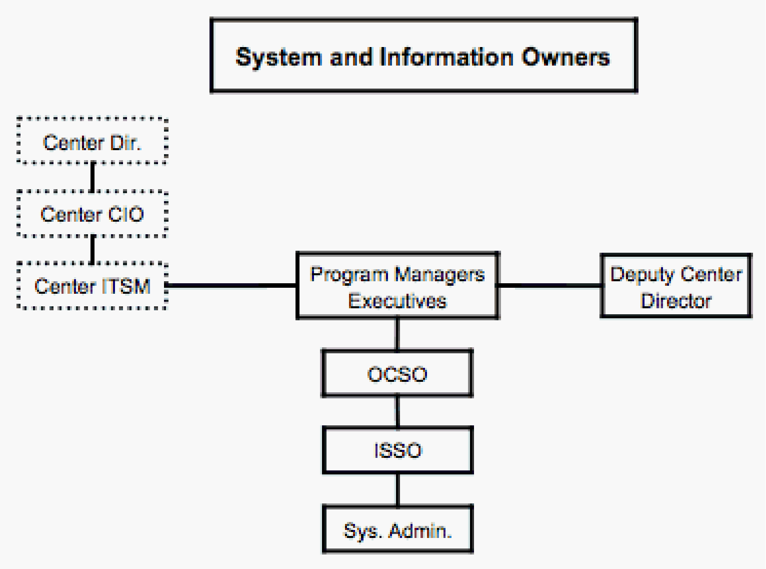


Figure 2-2 IT Security System and Information Owners

2.3.2 Project/Program/Functional Managers as Information System Owners

2.3.2.1 Every IT system has an information system owner who is responsible for the successful operation and protection of the system and its information. Program, project, and functional managers are often identified as the information system owners. Information system owners are usually civil service personnel; but can be support service contractors or partners under agreements with NASA. In addition, there can be information owners who entrust their information and applications to information system owners to process, store, and handle. Information system owners and information owners are responsible for ensuring that the system development life cycle (SDLC) security requirements are identified during the system's initiation phase, addressed throughout design reviews, tested and verified during implementation and operational phases, and maintained during the disposition phase.

2.3.2.2 A civil service manager shall oversee the IT security of the systems or applications that are operated and managed through a support service contract, contractor, grant, or agreement. For government-owned contractor-operated (GOCO) facilities (e.g., Jet Propulsion Laboratory), a non-civil service individual, at an equivalent civil service management level, may serve as the on-duty line manager.

2.3.2.3 Information System Owners (i.e., Program and Project Managers or their designee) shall:

a. Ensure that their system complies with the mandatory requirements of NPR 7120.5, NASA Program and Project Management Processes and Requirements, and with the IT security requirements controls to ensure protective safeguards are addressed early and throughout the system's life cycle.

b. Report systems costing more than $500,000 on the Center's "Capital Asset Plan and Business Case," Exhibit 300.

c. Ensure that the project and program plan, where applicable, integrates security throughout the life cycle, including the processes and procedures of NPR 7120.5, NASA Program and Project Management Process and Requirements.

d. Ensure their systems are designed and implemented in accordance with the NASA Enterprise Architecture.

e. Work with all their Information Owners, following the NIST guidance in developing the contingency requirements for their systems.

f. Ensure their systems comply with the C&A requirements identified in Chapter 14, System Certification and Accreditation, and provide adequate resources to meet these C&A requirements.

g. Ensure that all interconnected systems (i.e., systems owned by another organization) have an Interconnection Memorandum of Understanding (MOU) and Interconnection Security Agreement in place, which define the rules of behavior and controls that must be maintained for system interconnection and that these are included in the IT SSP.

h. Oversee the overall compliance of their assets with their defined/identified security requirements by ensuring that proper ITS controls are in place.

2.3.3 Information Owners

2.3.3.1 All NASA information has an owning organization responsible for its confidentiality, integrity, and availability. Although Information Owners may have their information processed by another organization, support service contractor, or partner, the NASA Information Owners shall be ultimately accountable and responsible for understanding any risk that another manager has accepted for the system processing their information.

2.3.3.2 Information owners shall:

a. Understand the IT security strategy, contingency requirements, and security risks of systems that process, store, and handle their information.

b. Be responsible for a program or function (e.g., procurement or payroll) including the supporting IT resources and provision of appropriate management, operational, and technical controls. This includes the information supporting a program or function regardless of whether the information is processed by another organization or contractor.

c. Play an essential role in IT security relative to strategic planning initiatives and be intimately aware of functional service requirements of the system supporting their information.

d. Ensure programmatic IT security interests are addressed during the IT security services life cycle.

e. Oversee the overall compliance of their assets with their defined/identified security requirements.

f. Concur or non-concur on the C&A decisions.

g. Retain the accountability and responsibility by ensuring rules of behavior are propagated that protects their information even when the information is shared with other organizations.

h. Ensure that all interconnected systems are documented and have signed agreements in place in accordance with NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, and Chapter 9, System Interconnectivity.

2.3.4 Organization Computer Security Official

2.3.4.1 An Organization Computer Security Official (OCSO) is responsible for a particular organization's IT Security Program. The OCSO serves as the critical communication link to and from that organization and its programs for all IT security matters.

2.3.4.2 The OCSO shall:

a. Serve as the organization's representative to the Center ITSM, representing the organization's director or office chief on all IT security matters and advising the Center NCCB on the possible impact from modifications in the IT network infrastructure.

b. Periodically report the status of the organization's IT security posture and concerns to the Center ITSM and the organization's senior manager.

c. Ensure the organization complies with NASA and Center IT security requirements, and notify the Center ITSM if there is an obstacle to meeting requirements, deadlines, or metrics.

d. Review annually the IT SSPs for the organization's systems identifying any changes that would require an update, such as changes in personnel, software and hardware, function, categories of information, information ownership, or risk, and verify the viability and the date of the last test of the contingency plan.

e. Report suspected and actual IT security incidents to the Center ITSM and line management, in accordance with Center-established incident response procedures.

f. Ensure compliance with OSPP requirements for media sanitization by the establishment of a process to ensure that storage media is purged of any data or information that has not been approved for public release prior to releasing the media outside the Center's control.

2.3.5 Information System Security Official

2.3.5.1 The information system security official (ISSO) is the principal staff advisor to the information system owner on all matters involving the IT security of the information system. This responsibility may also include physical security, personnel security, incident handling, and security training and education. For smaller systems, a system administrator may perform the ISSO role as well as the system administrator role.

2.3.5.2 The ISSO shall:

a. Ensure the security of an information system throughout its life cycle.

b. Play an active role in developing and updating the security plan for the information system as well as in managing and controlling changes to the system and assessing the security impact of those changes.

c. Cooperate in the development and implementation of security tools and mechanisms and other techniques consistent with NASA and Center standards to mitigate vulnerabilities for which there is no countermeasure.

d. Perform annual self-inspections of their systems and report the findings to their line managers, information system owner, and the cognizant OCSO.

e. Conduct system vulnerability checks to ensure that known vulnerabilities and exploits are identified and corrected and that residual risks are documented.

f. Periodically use tools to verify and/or monitor compliance with the NASA password policy for systems under their authority.

g. Ensure effective and timely incident reporting of all incidents and suspected incidents in accordance with Center procedures.

2.3.5.3 ISSO shall ensure appropriateness of user accounts by:

a. Ensuring that all users, administrators, and operators complete an account request document, which is approved by a NASA management official responsible for the individual (e.g., manager, sponsor, task manager) and by the line manager responsible for the system.

b. Promptly disabling access to a user's account if the user is identified as having left the Center, changed assignments, changed contracts, completed work on a grant or other agreement, or no longer requires system access.

c. Granting accounts only to individuals who have had the appropriate personnel screening in accordance with NPR 1600.1, NASA Security Program Procedural Requirements.

d. Ensuring that foreign nationals have approval by the CCS in coordination with the Center CIO, the Export Control Officer, and the information system owner prior to being granting access. Approval is required for access to every system.

e. Granting privileged, limited privileged, or non-privileged access to each system by foreign nationals or foreign representatives only with the written concurrence of the Center's Chief of Security and the information system owner.

2.3.6 System Administrator

2.3.6.1 NASA civil service and support service contract system administrators are the managers and technicians who design and operate information technology resources for their respective NASA

Centers. They are often a part of a larger Information Resources Management (IRM) organization. They usually have privileged access to NASA information resources.

2.3.6.2 Each system administrator shall:

a. Ensure that security controls, as described in the SSP, are properly implemented throughout the system's life cycle.

b. Maintain configuration profiles of all systems controlled by the organization including, but not limited to, mainframes, distributed systems, microcomputers, and dial-up and wireless access ports.

c. Implement all system changes required to protect their systems, including system patches as soon as they are available and tested to remove vulnerabilities. Systems, which are under a launch or mission freeze, must address this requirement immediately following the lifting of the freeze.

d. Monitor system integrity, protection levels, and security-related events; resolve detected security anomalies associated with their information system resources; conduct security tests as required; and assess and verify the implemented security controls.

e. Follow the Center's incident response procedures.

f. Be certified by the NASA System Administrator Certification Program in the particular operating system(s) for which they are responsible and in network and internet security practices.

g. Place the NASA CIO-approved warning banner on all systems that are owned by or operated on behalf of NASA.

2.4 Center IT Security Supporting Functions

IT security supporting functions are those functional roles that have a responsibility in ensuring that IT security policies, procedures, and requirements are implemented in their area of accountability. See Figure 2-3.

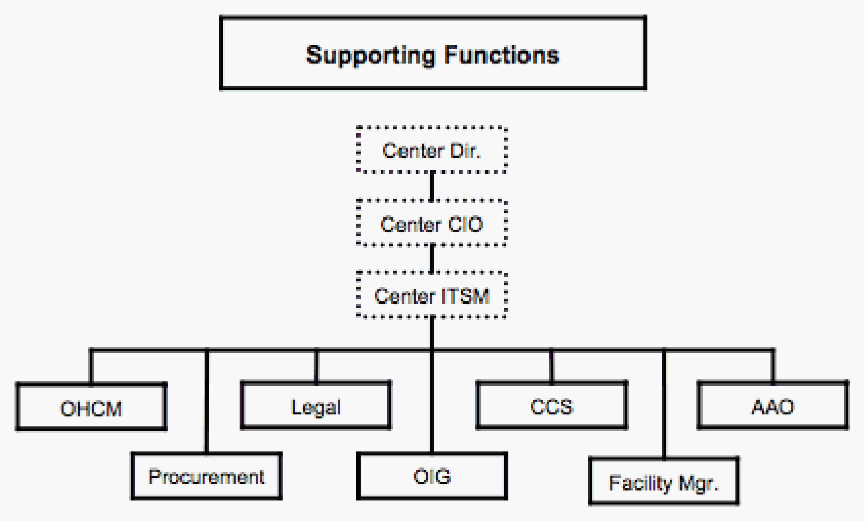


Figure 2-3 Center IT Security Supporting Functions

2.4.1 Head, Office of Human Capital Management

2.4.1.1 A partnership exists between the Office of Human Capital Management (OHCM) and the NASA CIO to further IT security curriculum development and the delivery of training for civil servants, including required training for support service contractors.

2.4.1.2 The Head of OHCM shall:

a. Ensure that all new civil service employees receive IT security awareness training prior to being released to their supervisor.

b. Ensure that all civil service employees assigned to management positions complete IT security awareness training for managers prior to assuming duties as a manager.

c. Advise management on administrative actions available for non-compliance with mandatory IT security requirements.

d. Work closely with managers and the CCS on issues involving the determination of position sensitivity and degrees of background investigations required for a particular position.

e. Provide security-related exit procedures when employees leave a NASA organization.

2.4.1.3 Head, Center's Training Office shall:

a. Provide reports quarterly to the Center CIO, Center ITSM, and the IT Security Awareness and Training Center on the status of employee training metrics.

b. Maintain records of civil service personnel who have taken training.

c. Maintain a schedule of when follow-on training will be required.

d. Track the status of employee training metrics.

e. Budget funds and resources for both initial and follow-on Center-specific IT security curricula.

2.4.2 Procurement Officers

2.4.2.1 The Procurement Officers are responsible for ensuring that solicitations and procurement and non-procurement instruments incorporate Federal and NASA clauses and provisions. Joint processes, developed in coordination with the SAISO and the ITSO, shall be established for verifying that IT security is specifically addressed in the initiation of solicitations and procurement and non-procurement instruments.

2.4.2.2 Procurement Officers shall:

a. Verify that NASA IT security requirements, as identified in the NASA FAR Supplement, are included in solicitations and procurement and non-procurement instruments or specifically documented as not being appropriate by the funding organization.

b. Direct those initiating contracts and other solicitations and procurement and non-procurement instruments to their CIO and ITSM for assistance in documenting the information security category and understanding the resulting impact level, required security controls, and budget considerations.

2.4.3 Contracting Officers Technical Representative (COTR)

2.4.3.1 The COTR shall:

a. Obtain the advance coordination of the cognizant ITSM of the issuance of contract modifications or new task orders, which will involve operation, use, or access to Federal or NASA IT resources or information.

b. Establish a process for notifying the Center Account Authorization Official (AAO) and the Center ITSM when any contractor employee is terminated or otherwise no longer requires system access.

c. Establish processes to verify that all contractor employees complete the require IT security awareness training, as specified in the contract, prior to being granted access to NASA IT systems, information, or data.

d. Work closely with system owner and the CCS when determining the position sensitivity and the required degrees of background investigations required for all contractor positions. (See Chapter 4, Section 4.5 of NPR 1600.1, NASA Security Program Procedural Requirements, for more information.)

2.4.4 General Counsel

2.4.4.1 The General Counsel shall:

a. Advise the CIO regarding IT security policies and provide procedures for legal compliance.

b. Provide managers with legal advice regarding non-compliance with IT security policy.

c. Be responsible for advising the acquisition team on legal issues associated with the procurement.

2.4.4.2 The General Counsel shall review and approve non-disclosure agreements to ensure they are consistent and to ensure they provide adequate protection for NASA ACI/SBU information.

2.4.5 Center Chief of Security

2.4.5.1 The Center Chief of Security (CCS) shall:

a. Conduct appropriate personnel security screening for those working in high impact or critically sensitive positions, which includes those who can bypass IT technical security controls and processes.

b. Coordinate, investigate, and approve requests for foreign nationals and international partners who require privileged or non-privileged access to systems, applications, and networks operated by or on behalf of NASA.

c. Develop a process that alerts the appropriate account management officials and the organization ISSO or OCSO of persons having access to IT information and resources leaving employment and exiting the Center.

d. Ensure the physical security of Center IT resource facilities.

2.4.5.2 The CCS, in coordination with the OSPP CI Officer, shall establish a process to gather intelligence information regarding threats toward IT resources and provide this information to the Center ITSM and the CIO. The Center CIO shall ensure that the information system owner is informed.

2.4.5.3 The CCS shall approve access to IT resources, in accordance with NPR 1600.1, NASA Security Program Procedural Requirements, for all foreign nationals.

2.4.6 Office of Inspector General

2.4.6.1 The Office of Inspector General's (OIG's) role in IT security is to investigate computer crimes for possible prosecution in court and to conduct audits of IT resources for proper management, which includes appropriate protective controls. In this role, the OIG shall:

a. Promptly notify appropriate NASA management of incidents whenever the OIG has reason to believe, or is aware, that there is a threat to human safety or critical missions.

b. Coordinate, to the greatest extent practicable, with the Center CIO and ITSM, when use of Center computer or network data is needed to support an investigation that is being conducted.

c. Investigate, as appropriate, incidents forwarded by the Center ITSM, which constitute a computer crime.

d. Serve as the focal point for referrals to the Department of Justice and other external law enforcement organizations of all violations of Federal criminal and civil statutes related to computer system intrusions or criminal misuse of computers.

2.4.7 Building or Facility Manager

2.4.7.1 Building or facility managers are responsible for ensuring the provision of such services as electrical power and environmental controls necessary for safe and secure system operations. Often, separate medical, fire, hazardous waste, or life safety personnel augment these managers.

2.4.7.2 Building or facility managers shall:

a. Ensure that physical access controls protecting information systems are correctly installed, maintained, and tested annually.

b. Ensure that safety controls are managed and tested annually.

c. Ensure that HVAC controls are adequate for IT system availability requirements, are maintained, and are tested.

d. Support the certification of IT security controls. Security controls are the management, operational, and technical controls prescribed for information contained in an information system which, when taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and the information.

2.4.8 Center Account Authorization Official

2.4.8.1 The Center Account Authorization Official (AAO) serves as the primary technical representative for account management issues and provides guidance and oversight of the daily activities of all Center staff supporting the NASA Account Management System (NAMS).

2.4.8.2 Center AAOs shall:

a. Have the authority and responsibility for all aspects of policy, business operations, and operational life cycle for NAMS.

b. Provide guidance and oversight of the account management activities.

c. Enforce NIST SP 800-53, Recommended Security Controls for Federal Information Systems, and NASA security controls and requirements for NAMS passwords.

d. Work with the Center ITSM on security issues, compliance, and support.

e. Report known or suspected security incidents to the Center ITSM, in accordance with Center procedures.

2.4.9 User Community and NASA Customers

2.4.9.1 Because NASA resources, information, data, and processing systems are held in public trust, the NASA user community and NASA customers share responsibility for protecting these IT resources. Policies and requirements cannot always be implemented through automated technical controls. Consequently, individuals shall voluntarily comply with procedures by agreeing to accept NASA's Appropriate Use Policy Statement (See Section 11.3.3, Appropriate Use of IT Resources).

2.4.9.2 Users of NASA systems or information shall:

a. Comply with the requirements for limited personal use and inappropriate use described in Section 11.3.4, Limited Personal Use of IT Resources. If users are unsure about whether an activity is permitted, they should consult with their Center ITSM.

b. Comply with existing laws and policies that restrict the distribution of ACI and SBU information. (See the procedures described in NPR 1600.1, NASA Security Program Procedural Requirements.)

c. Be responsible for ensuring their sponsored guests and visitors are aware of Center policies, procedures, and requirements regarding the use of NASA IT resources, including wireless access.

d. Comply with NASA password policies as described in Section 11.3.7, Password Requirements, and NASA incident handling policies and procedures as described in Chapter 17, Security Incident Handling and Reporting.

e. Users of NASA information systems or those having access to NASA information shall immediately report any known or suspected IT security incidents, following the Center's procedures for incident reporting. It is the responsibility of the OCSO or information system owner to notify the Center ITSM of all known or suspected incidents.

f. Complete mandatory basic IT security awareness training prior to accessing NASA systems and applications and annually thereafter as long as access to NASA information or IT resources continues.

2.5 Certification and Accreditation Roles

2.5.1 The role of the Agency Authorizing Official in the accreditation process is detailed in Section 14.5, Accreditation Process Requirements.

2.5.2 Authorizing Official (AO) Requirements

2.5.2.1 The AO is the NASA management official with the authority to approve the operation of the information system at an acceptable level of risk to NASA operations (including mission, functions, image, or reputation), agency assets, or individuals.

2.5.2.2 The AO, by relying on themselves or IT security professionals, shall:

a. Be knowledgeable in computer, telecommunications, and networking technology, as well as security methods and practices. NASA will provide role-based AO training.

b. Have the authority to:

(1) Oversee the budget and business operations of the information system within the NASA organization and have the authority to allocate resources to achieve an acceptable level of security, to remedy security deficiencies, or to halt processing.

(2) Approve security requirements documents, security plans, memorandums of agreement (MOA), memorandums of understanding (MOU), and any authorized or allowable deviations from security policies.

(3) Allocate resources to achieve an acceptable level of security.

(4) Remedy security deficiencies.

(5) Halt processing when conditions warrant.

c. Assume responsibility and accountability for the risks of operating the information system in a specific environment through the completion of the accreditation process and be accountable for both the system and for adverse impacts to NASA if a breach of security occurs.

d. Ensure the C&A process is performed during life cycle changes of systems, when a significant change is determined to affect security, and at least every three years prior to the expiration of the last C&A.

e. Establish the minimum baseline security controls for their IT security systems.

f. Ensure that the C&A process is followed prior to granting a full Authorization to Operate (ATO) or an Interim Authorization to Operate (IATO). This includes when a significant change is determined to affect security and at least every three years prior to the expiration of the last C&A.

g. Grant one of three types of accreditation decisions, which are more fully explained in Section 14.4, Accreditation Process, upon completion of the C&A process:

(1) Authorization to operate the system once the certification process has been completed.

(2) Issue an IATO to operate the system under specific terms and conditions.

(3) Deny authorization to operate the system (or if the system is already operational, halt operations) if unacceptable security risks exist.

h. Require information system owners whose systems have interim accreditations or operational denial to provide documentation on the corrective actions to be taken and the timeline for completion in order to achieve full accreditation or to resume operations.

i. Establish agreements among the AOs, if multiple AOs are involved, and document in the security plan.

2.5.2.3 Authorizing Officials for master system plans shall:

a. Make the security accreditation decisions for their master systems which establish the IT security posture of the master and their subordinate systems.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA CFO, NASA CIO, and applicable program office that funding be redirected to implement security controls required for master or subordinate systems to achieve full ATO.

d. Concur or non-concur on the determination of a master system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls which will be inherited by any subordinate system under the authority of the master system.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.5.2.4 Authorizing Officials for subordinate systems plans shall:

a. Make the security accreditation decisions for the subordinate systems, which establish the IT security posture of the subordinate system and explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

b. If necessary, advocate to the NASA CFO, NASA CIO, and applicable program office that funding be redirected to implement security controls required for the subordinate systems to achieve full ATO.

c. Concur or non-concur on the system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls inherited from the master system. Non-concurrences shall indicate that the system needs to be aligned with a different master system or that a new master system must be created.

d. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

e. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.5.3 Certification Agent Requirements

2.5.3.1 The independence of the Certification Agent (CA) is an important factor in assessing the credibility of the security test and evaluation results and ensuring that the AO receives the most objective information possible in order to make an informed, risk-based security accreditation decision.

2.5.3.2 The CA shall be appointed to preserve the impartial and unbiased nature of the security certification as follows:

a. For high and moderate impact systems, the Agency independent third-party shall be identified by the SAISO with concurrence by the OSPP.

b. For a low impact level system, the CA can be selected from the system support staff.

2.5.3.3 The Certification Agent shall:

a. Provide an independent assessment of the security plan to ensure the plan provides a complete and consistent security specification for the information system, prior to initiating the security test and evaluation activities.

b. Conduct a comprehensive assessment of the management, operational, and technical security controls of the information system to determine the effectiveness of those controls in a particular environment of operation and the vulnerabilities in the system after the implementation of such controls. A comprehensive assessment means the review and analysis of all the security controls identified as "baseline security controls for the impact level" as identified in SP 800-53 shall be reviewed and analyzed.

c. Review the results of testing of selected security controls, summarize results, and identify residual risks and impacts.

d. Provide recommended corrective actions to reduce or eliminate vulnerabilities in the information system.

e. Prepare an Accreditation Package consisting of a Certification Letter of Recommendation, a Risk Assessment Summary, and an IT SSP for the AO.

f. Be supported by a certification team providing the essential assessment capabilities necessary to complete the evaluation of the security controls, depending on the size and complexity of the information system and NASA's requirements.

Chapter 3 IT Program and System Security Assessments

3.1 IT Program and System Security Assessments Overview

3.1.1 FISMA requires NASA to conduct annual IT security assessments of systems and programs and reviews of Centers and contractor operations or facilities that process, store, or handle NASA information, and parties under grants, agreements, or partners via volunteer or special agreements that process, store, or handle NASA information.

3.1.2 A "contractor operation or facility" is an entity under contract or other government agreement that processes or stores NASA information or data and is managed by the entity with little government technical oversight of its operations. This includes, but is not limited, to a government-owned, contractor-operated (GOCO) facility, an outsourced function, a grant, or agreement from NASA to a college, university, or research facility to process, use, or be afforded access to Federal or NASA information or data.

3.2 IT Program and System Security Assessment Requirements

3.2.1 All IT program and system security assessments shall be coordinated with managers at the appropriate level (i.e., the NASA OCIO, Center CIO, Center ITSM, or the Procurement Officer) to ensure that critical business and mission functions are not disrupted and contractual provisions provide for assessments in place.

a. All non-NASA systems containing NASA information that is categorized as having high impact to the NASA mission or operations shall have an assessment completed once every fiscal year under the oversight of the NASA CIO or Center CIO, as appropriate.

b. All NASA information system owners shall ensure that the appropriate reviews and testing as called for by NIST are conducted.

3.2.2 The necessary depth and breadth of an annual program or system assessment shall follow ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment, and ITS SOP-0017, IT Security Penetration Test Plan and Rules of Engagement.

3.2.3 Non-NASA performed IT program and system security assessments shall have an assessment that provides for:

a. Personnel screening equivalent to the information system's most stringent screening requirement, per NPR 1600.1, NASA Security Program Procedural Requirements, for all assessment team members.

b. Non-disclosure agreements previously approved by NASA General Counsel or Chief Counsel, to be signed by all entities and personnel participating in the assessment.

c. Protective controls for all materials, documents, working papers, and assessment findings at a level equivalent to that required by the information category.

d. The return or destruction of all materials, documents, working papers, and assessment findings at the completion of the IT program or system security assessment.

e. The assessment plan authorized and signed by the government sponsor of the assessment and the program manager of the non-NASA certifying entity responsible and accountable for the assessment prior to the start of the assessment.

3.2.4 Penetration testing conducted as part of any assessment shall adhere to ITS-SOP-0017, IT Security Penetration Test Plan and Rules of Engagement.

3.2.5 Federal and NASA non-compliance findings, which are not corrected or waived during the assessment, shall be entered into the program's or IT system's POA&M and be reported to the cognizant Contracting Officer and AO. The requirement to report non-compliance of a contractor's system shall be reported to the responsible civil service manager as well as all NASA Information Owners.

3.3 Additional IT Program and System Security Assessment References

a. OMB M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act.

b. NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems.

c. ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment.

d. ITS SOP-0017, IT Security Penetration Test Plan and Rules of Engagement.

e. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

Chapter 4 Contracts, Grants, and Agreements

4.1 Contracts, Grants, and Agreements Overview

4.1.1 NASA shall refer to NIST SP 800-64, Security Considerations in the Information System Life Cycle, Appendix B for guidance on specifications, clauses, and appropriate text for contracts, grants, agreements, purchase orders, purchase-card buys, and inter-governmental orders.

4.1.2 Since FISMA applies to both information and information systems used by NASA, its support service contractors, and other organizations and sources, it has somewhat broader applicability than that of prior security laws. Therefore, the NASA IT Security Program and its requirements apply to all organizations (i.e., sources) which possess or use Federal or NASA information or which operate, use, or have access to Federal or NASA information systems on behalf of NASA. Such organizations include support service contractors, grantees, state and local governments, industry partners, partners under Space Act Agreements, International Partners, and agreements with universities and other educational entities and special volunteer partners whether funded or not funded.

4.2 Contract Instruments

4.2.1 The appropriate depth and breadth of security controls shall be documented in specific clauses and determined by the following factors:

a. The potential risk and magnitude of harm to the program, system, or information.

b. The complexity of the information systems including networked capabilities, number of users, and interconnected dependencies.

c. The category and impact of the information, background screening requirements for access to the information, and redistribution restrictions governing the information.

d. The adequacy and successful implementation of the POA&M process for correcting weaknesses in the system or program.

4.2.2 Clauses containing information and information system security requirements shall apply to all sub-contractors and all out-sourced IT services.

4.2.3 Clauses that identify information and information system security controls requirements shall be included in all solicitations and procurement and non-procurement instruments.

4.2.4 A contract clause shall be included to apply specific security controls to equipment that is acquired by a Federal contractor incidental to a Federal contract when Federal or NASA information is processed, stored, or handled within incidentally-acquired equipment.

4.2.5 A contract clause shall be included to detail NASA's specific authority and limitations to conduct IT security reviews and conduct investigation of suspected non-compliance with specified security controls and computer crimes.

4.2.6 A contract clause shall be incorporated requiring that all system administrators be certified in accordance with the NASA System Administrator Certification Program for the operating system(s) for which they are responsible.

4.2.7 Proposal evaluations and source evaluation boards shall have information and information system security as a critical element in the Mission Suitability (MS) Technical Approach (Subfactor-2) . 4.2.8 Contract instruments shall stipulate that the contractor delivers an IT Security Program Plan that describes the processes they utilize that are commensurate with NASA IT security requirements for protecting NASA information contained within their corporate systems, as well as meeting NPR 2810.1 requirements when the contractor is operating or managing NASA systems. Contents for this plan can be found in ITS-SOP-0018, Contract IT Security Program Plan Procedures.

4.3 Grants, Cooperative Agreements, and Special Volunteer Program Instruments

4.3.1 Grants, cooperative agreements, and special volunteer program instruments that are conducting basic research utilizing publicly-available data are required to use this document solely as guidance to ensure that that IT security best practices are used.

4.3.2 Grant, cooperative agreement, and special volunteer program instruments with the requirements listed below shall utilize the language in the IT Security clause(s) to ensure security is appropriately addressed. The requirements are:

a. Utilizing ACI or SBU information, proprietary information.

b Performing remote control of space-based or sub-orbital assets.

c. Requiring hosting systems on NASA IP address space.

4.4 Additional Contract, Grant, and Agreement Instruments References

a. NIST SP 800-35, Guide to IT Security Services.

b. NIST SP 800-36, Guide to Selecting Information Technology Security Products.

c. NIST SP 800-64, Security Considerations in the Information System Life Cycle.

Section II Defining The System

a. Many activities are involved in the design and implementation of an information system. Successful protection of IT resources relies upon program-level IT security requirements and system-level security requirements. Program-level IT security requirements are general in nature and apply to overarching concepts. System-level security requirements are specific management, operational, and technical security controls and processes utilized to certify and accredit a system for processing information.

b. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, provides additional guidance on the IT security system life cycle and the criticality of including IT security considerations at all stages in the life cycle. The implementation of IT Security (ITS) practices is not a linear process. While there is a general flow from the initiation of an IT system through its life cycle to disposal of the system, several of the critical IT security processes are not linear, but are cyclical or can be repeated in whole or in part throughout the system's life cycle.

Chapter 5 System Development Life Cycle

5.1 System Development Life Cycle Overview

5.1.1 Information and information systems, like programs and projects, have a life cycle. NIST defines the SDLC phases as: (1) initiation, (2) acquisition and development, (3) implementation, (4) operations and maintenance, and (5) disposal.

5.1.2 Information and IT security controls are critical to IT investments and systems being certified and accredited to operate during development testing, proof-of-concept testing and operations, and pilots, as well as operational status. To ensure that the C&A of systems is successful without affecting schedule, cost, and performance, IT security controls shall be planned for and factored into all decisions during the life cycle processes.

5.1.3 The NPR 7120.5 life cycle and the life cycle documented in NIST SP 800-64, Security Considerations in the Information SDLC, are complementary.

5.2 System Development Life Cycle Requirements

5.2.1 IT security controls shall be planned for and factored into all decisions during the SDLC processes including relevant program and project IT requirements and during the SDLC of any applicable program or project IT resources. IT security must be considered throughout the SDLC, which goes from conception to disposal.

5.2.2 To ensure that IT security is integrated into the SDLC initiation phase and following NPR 7120.5, NASA Program and Project Management Processes and Requirements, all program Formulation Authorization Documents (FADs) shall identify the FIPS 199 information type that IT investments and systems will be processing and handling.

5.2.3 NASA shall avoid impacts to schedule, cost, and performance during the SDLC acquisition and development phases of PCAs by:

a. Designing information systems that comply with Federal laws and NASA IT security requirements.

b. Identifying, by title, the NASA authority authorized to grant exceptions to Federal laws and NASA IT security requirements.

5.2.4 To ensure that the SDLC implementation, operations and maintenance, and disposal phases, including the transition from a development/proof-of-concept to operational status, projects must:

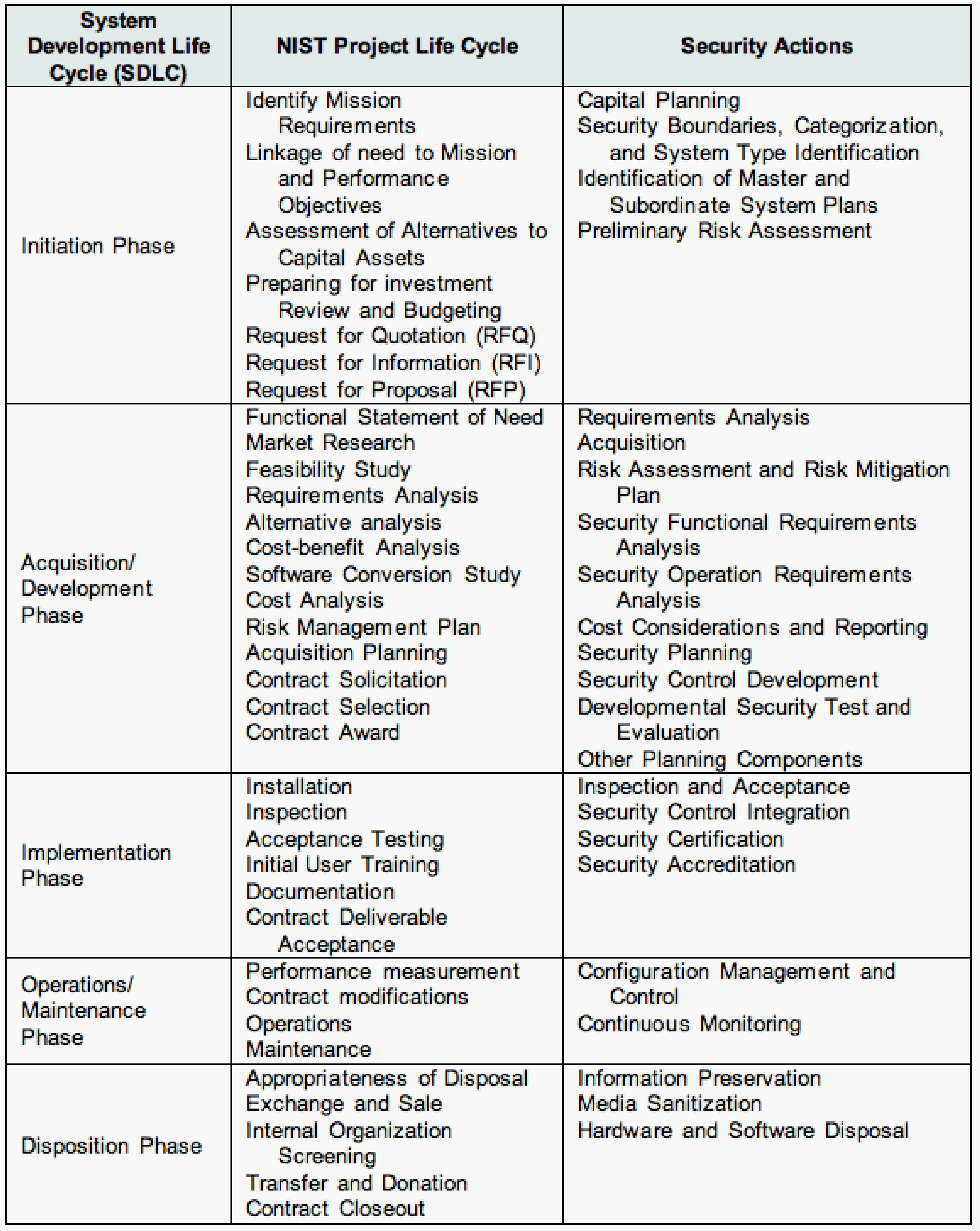
a. Incorporate system security planning, including risk assessment, contingency planning and testing, C&A, and continuous monitoring early in the system formulation and throughout the life cycle of the processes and procedures of NPR 7120.5, NASA Program and Project Management Process and Requirements, which complement the IT security life cycle processes.

b. Identify the category of the information expected to be accessed or created.

c. Specifically assign an ISSO responsible for ensuring the information system complies with Federal and NASA IT security requirements.

d. Include IT security costs.

5.2.5 Figure 5-1 lists the various NIST SDLC phases, project life cycle, and security actions. This figure demonstrates how the same security control process is addressed in multiple life cycle phases. See NPR 7120.5 for NASA's life cycle phases.



System Development Life Cycle (SDLC)	NIST Project Life Cycle	Security Actions
Initiation Phase	Identify Mission Requirements Linkage of need to Mission and Performance Objectives Assessment of Alternatives to Capital Assets Preparing for investment Review and Budgeting Request for Quotation (RFQ) Request for Information (RFI) Request for Proposal (RFP)	Capital Planning Security Boundaries, Categorization, and System Type Identification Identification of Master and Subordinate System Plans Preliminary Risk Assessment
Acquisition/ Development Phase	Functional Statement of Need Market Research Feasibility Study Requirements Analysis Alternative analysis Cost-benefit Analysis Software Conversion Study Cost Analysis Risk Management Plan Acquisition Planning Contract Solicitation Contract Selection Contract Award	Requirements Analysis Acquisition Risk Assessment and Risk Mitigation Plan Security Functional Requirements Analysis Security Operation Requirements Analysis Cost Considerations and Reporting Security Planning Security Control Development Developmental Security Test and Evaluation Other Planning Components
Implementation Phase	Installation Inspection Acceptance Testing Initial User Training Documentation Contract Deliverable Acceptance	Inspection and Acceptance Security Control Integration Security Certification Security Accreditation
Operations/ Maintenance Phase	Performance measurement Contract modifications Operations Maintenance	Configuration Management and Control Continuous Monitoring
Disposition Phase	Appropriateness of Disposal Exchange and Sale Internal Organization Screening Transfer and Donation Contract Closeout	Information Preservation Media Sanitization Hardware and Software Disposal

Figure 5-1 Life Cycle Phases and other IT Security Elements

5.3 Additional System Development Life Cycle References

a. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.

b. NPR 7120.5, NASA Program and Project Management Process and Requirements.

Chapter 6 Information and Information System IT Security Strategy

6.1. In the development of an SSP, the information and information system owner shall document the information and information system strategy. A system strategy provides a high-level description of how the system operates, which includes a high-level design schematic of the system and corresponding security characteristics of the system such as types of data, user communities, interconnectivity, and data flows (i.e., who and how users will interact with the information, how information will move between locations and users) and the desired information management goals and objectives.

6.2 Information security covers not just information but all infrastructure that facilitates its use such as processes, systems, services, technology, etc., and including computers, voice, and data networks. NASA is required to develop an IT security strategy in the initiation phase for each system that lays out the end-to-end IT security, which is defined as "safeguarding information from point of origin to point of destination." The vision is that security needs to possess an end-to-end property, otherwise security breaches are possible at the interfaces, which can result in building gaps. This type of strategy can significantly streamline the design process since it supports a variety of resource-specific considerations early on in the system's IT security life cycle. By establishing and maintaining a unifying vision and strategic direction, the information system owner can ensure that through each phase of the IT security life cycle that the protection of the information and information system is being met. This means that the information system owner needs to refer continually back to the IT security strategy as the system moves through the IT security life cycle to ensure that the strategy is being implemented and that the strategy itself is still valid.

6.3 No one can ever eradicate all risk of improper or capricious use of any information. The level of information security sought in any particular situation should be commensurate with the value of the information and the loss, financial or otherwise, that might accrue from improper use (i.e., disclosure, degradation, denial, etc.). The strategy should capture these choices.

Chapter 7 System Characterization, Information Categorization, System Types, and System Boundaries

7.1 System Characterization

7.1.1 The characterization of a system is based on: the categorization of its information and impact level, the designation of the system type, and identification of its system boundaries. The activity of characterizing the system can sometimes be a lengthy process as different requirements are sorted out.

7.1.2 All three elements in the system characterization process should be considered together. These characteristics will determine the system security controls.

7.2 Categorization of Information

7.2.1 To determine the potential impact to an information system and the level of security required to manage risk to an acceptable level, the information itself must be analyzed for its three IT security objectives and the impact each would have on the mission or functional line of business. The result of the analysis is an "IT security category." The methodology for the categorization of information is documented in the FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems. The security objectives are defined as:

a. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

b. Integrity. Guarding against unauthorized information modification or destruction, which includes ensuring information non-repudiation and authenticity. Loss of integrity is the unauthorized modification or destruction of information.

c. Availability. Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

7.2.2 For each security objective there are levels of potential impact which must be considered. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or availability of the information or information system would have on NASA operations, including mission, functions, image, or reputation, NASA assets, or individuals (including privacy considerations). The potential impact analysis should focus on the risk to the mission or functional line of business. (See FIPS 199, Table 1 for a detailed explanation of potential impacts for confidentiality, integrity, and availability). The levels of potential impact are:

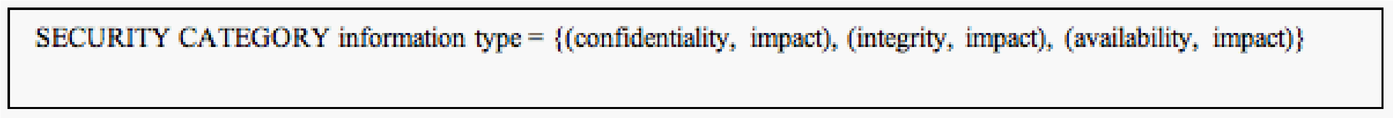
a. Low. The potential impact is considered low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on NASA operations, organizational assets, or individuals.

b. Moderate. The potential impact is considered moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on NASA operations, organizational assets, or individuals.

c. High. The potential impact is considered high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on NASA operations, organizational assets, or individuals.

d. Not applicable. The potential impact is considered not applicable if the loss of confidentiality has no impact (because the information is already in the public domain). Integrity and availability are never considered not applicable.

7.2.3 An information system may be intended to process, handle, or store many types of information such as privacy information, budget information, research data, public affairs information, capital planning, inventory data, and human resource information. Each type of information shall be analyzed for the potential impact to its confidentiality, integrity, and availability. Establishing an appropriate security category for an information type requires determining the potential impact for each security objective associated with the particular information type. The generalized format for expressing the security category of an information type is shown in Figure 7-1.



SECURITY CATEGORY information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}

Figure 7-1 Security Category Expression

7.2.4 For any information system, the impact values assigned to the information system will be the highest value of the respective security objectives of confidentiality, integrity, availability. The "high water mark" will be selected from the security categories that have been determined for each type of information resident on the information system.

7.2.5 Acceptable values for the potential impact are low, moderate, or high. In the case of confidentiality, not applicable is an acceptable value for information that is available to the public already.

7.3 Categorization of Information Requirements

7.3.1 NASA shall follow the guidance in FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, for the categorization of information.

7.3.2 The SSP for a master system shall:

a. Identify the major information types, which will be processed, handled, or stored.

b. Document the highest impact value (i.e., low, moderate, high) for each IT security objective as the IT security category.

c. Justify any management determination that a different security category is more appropriate than the one recommended by NIST SP 800-60, Volume I and II, Guide for Mapping Types of Information and Information to Security Categories.

7.3.3 The SSP for subordinate systems shall:

a. Document the associated master system's determination of the IT security category and impact value, which are inherited by the subordinate system.

b. Provide justification for any site-specific, information system owner determination that a different category is more appropriate than the one recommended by the master SSP, either higher or lower.

c. Identify the result in the Accreditation Package.

d. Document the concurrence or non-concurrence of the Center CIO and the ITSM on the certification security assessment report.

7.4 Information Technology System Types

7.4.1 The NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, will assist in understanding the relationship between categorization and system types. The OMB Circular A-130, Appendix III requires that Federal information systems be categorized into two types of systems, major applications (MA) and general support systems (GSS). Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. In NPR 1600.1, NASA Security Program Procedural Requirements, 8.4, NASA Critical Infrastructure and Key Resources, NASA has elected to designate its critical infrastructure and key resources as Mission Essential Infrastructure (MEI) to better facilitate designation of vital "mission-oriented" critical infrastructure and key resources.

7.4.1.1 Major Application (MA). An MA system is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of, the information in the application. A breach in an MA has the potential to compromise many individual application programs and hardware, software, and telecommunications components. MA systems can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

7.4.1.2 General Support System (GSS). A GSS system is an interconnected information resource under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, facilities, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

7.4.1.3 NASA Critical Infrastructure and Key Resources--MEI Protection Program. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, directs agencies to establish a program to identify critical infrastructure and key resources, evaluate these assets for vulnerabilities, and fund and implement appropriate security enhancements (procedural and physical) to mitigate vulnerabilities. NASA has elected to designate its critical infrastructure and key resources as MEI to better facilitate designation of vital "mission oriented" critical infrastructure and key resources.

7.4.2 Information Technology System Types Requirements

7.4.2.1 All master system and subordinate owners shall work with their Center or Agency ITSM(s) to determine whether their master system or subordinate system is either a GSS or MA, as referenced in Guide for Developing Security Plans for IT Systems NIST SP 800-18, Guide for Developing Security Plans for IT Systems. Master and subordinate systems are addressed in Chapter 8, Master and Subordinate IT Systems.

7.4.2.2 Master systems shall be identified as either an MA system or a GSS. A Master, or "umbrella," system is one which provides an overall picture of the security of the systems under an Agency Deputy Mission Director's responsibility and is a key component of the certification and accreditation process. Master systems are supported by subordinate SSPs for individual systems.

7.4.2.3 Subordinate systems shall have the same IT system type (MA or GSS) as the associated master system. Subordinate systems support a master system. Certification testing of security controls is to be accomplished at the subordinate system level.

7.4.2.4 MEI systems shall be master systems identified as an MA or a GSS system.

7.5 System Boundaries

7.5.1 A system is defined by logical boundaries placed around a set of IT processes, communications, storage, and related resources, as well as any interdependence on other systems. The elements within these boundaries constitute a single system requiring a security plan. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems and NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems provide additional guidance. Assigning resources to an information system defines the security accreditation boundary for that system. C&A is required of all IT resources within the boundary and the security posture of any interdependencies identified, verified, and documented. The following factors (described in Chapter 6, Information and

Information System IT Security Strategy, Section 7.2, Categorization of Information, Section 7.3, Categorization of Information Requirements, and Chapter 8, Master and Subordinate IT Systems) shall be considered in assigning the system boundary: the categorization of information, the information system type, the assignment as a master or subordinate system, and the system's IT security strategy.

7.5.2 System Boundaries Requirements

7.5.2.1 IT system boundaries shall encompass IT resources:

a. Which are all under the same higher management authority.

b. Which perform the same mission or functional line of business.

c. Which have essentially the same operating characteristics and IT security category.

d. Which are interconnected or networked.

e. Which reside in the same general operating environment or in various locations with similar operating environments.

7.5.2.2 System boundaries shall be:

a. Defined and documented in the SSP for both master and subordinate systems.

b. Established prior to conducting the initial risk assessment.

c. Negotiated among the information system owner, the AO, the cognizant CIO, and the IAO.

7.5.2.3 Master system boundaries shall:

a. Have the same information security category for all systems under its accreditation authority.

b. Be coordinated with the OCIO to ensure the security accreditation boundary supports the NASA Enterprise Architecture.

c. Be subdivided into subordinate systems when the resources are large or complex or have dispersed local operational and security management.

7.5.2.4 Once the initial boundaries have been determined, the information system owner shall review Chapter 6, Information and Information System IT Security Strategy, to ensure that the system is still in line with the information and IT information system security strategy.

7.6 Additional System Characterization, Information Categorization, System Types, and System Boundaries References

a. OMB Circular A-130 Appendix III, Security of Federal Automated Information

Resources.

b. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

c. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook.

d. NIST SP 800-18, Guide for Developing Security Plans for IT Systems.

e. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

f. NIST SP 800-60, Volumes I and II, Guide for Mapping Types of Information and Information Systems to Security Categorization Levels.

g. NPR 1600.1, NASA Security Program Procedure Requirements.

Chapter 8 Master and Subordinate IT Systems

8.1 Designation of Master and Subordinate IT Systems

8.1.1 NASA has organized its IT systems with its programmatic and institutional lines of business to comply with OMB and FISMA reporting requirements on IT systems and the OMB and NIST criteria for defining a system's accreditation boundary of responsibility to align with the terms used within NASA Structure Management (NSM). By following NASA's lines of business, IT systems align (1) the budget authority with the information security AO; (2) the mission and functional responsibilities with system ownership and managing risk; and (3) the performance objectives with operational characteristics and security needs. Since managing information security is mandatory for all IT systems and since IT systems have various SDLCs, NASA has established master-level systems to allow Agency- and program-level information security controls to be certified and accredited for all subordinate systems under each master system's authority. A Master system's decisions and security controls are inherited by its subordinate systems.

8.1.2 Master systems can be comprised of a single MA or a MEI system. Master plans may also establish information security requirements for many subordinate GSSs. Designated AOs establish high-level master systems. Following the certification process, the AO accredits the system. (See Chapter 14, System Certification and Accreditation.)

8.2 Master and Subordinate IT Security Systems Requirements

8.2.1 Master SSPs shall:

a. Document the security posture of the master system including the IT security category, system type, the NASA-level security controls, the selection of subordinate system security controls, and contingency requirements which shall be certified and accredited prior to proof-of-concept testing, pilot deployments, or full operational status.

b. Be registered with the OCIO's IT System Registry.

c. Identify all subordinate systems under its authority in the SSP.

d. Track and document information regarding their subordinate systems including their C&A status, POA&M status, date of recertification and reaccreditation, the date of the last review of security controls, and the name of the information system owner.

8.2.2 Subordinate SSPs shall:

a. Document the inherited master system's IT security category, system type, NASA-level security controls, assessment of overall risk, and contingency requirements. If no master system has been established, the subordinate system shall make the interim security determinations.

b. Document the security posture of the system.

c. Document the results of the completed risk assessments for specific (i.e., local or site) risk and environmental conditions, since the results of the risk assessment conducted for the master system are inherited by the subordinate system. If no master system has been established, the subordinate system must complete a full system risk assessment.

d. Document the certification and accreditation decision which either a full or an interim ATO (IATO), prior to proof-of-concept testing, pilot deployments, or full operational status.

e. Be registered with the appropriate master system AO or OCIO, if a master system has not been established.

f. Track the C&A status, the POA&M status, the date recertification and reaccreditation is required, and the date of the last review of security controls.

8.3 Additional Master and Subordinate IT System References

a. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook.

b. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems.

c. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information.

Chapter 9 System Interconnectivity

9.1 Interconnected Systems

9.1.1 A system interconnection is defined as the direct connection of two or more IT systems for sharing data and other information resources. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, provides guidance for planning, establishing, maintaining, and terminating interconnections between IT systems that are owned and operated by different organizations.

9.1.2 NASA shall follow the NIST "life-cycle management" approach for interconnecting IT systems, with an emphasis on security. The four phases of the interconnection life cycle that are addressed in NIST SP 800-47 are: (1) Planning the interconnection, (2) Establishing the interconnection, (3) Maintaining the interconnection, and (4) Disconnecting the interconnection.

9.2 Interconnectivity Requirements

9.2.1 All NASA SSPs shall document written Interconnection Security Agreement(s), in accordance with NIST SP 800-47, System Interconnectivity, Appendix A, which documents the technical and security control requirements of the interconnection.

9.2.2 All NASA SSPs shall include, by reference or inclusion, an MOU/MOA, in accordance with NIST SP 800-47, Appendix B, which defines the participating parties' responsibilities. All MOU/MOA agreements for interconnecting systems shall contain technical and security control requirements per NIST SP 800-47 and the controls covered in the applicable SSPs.

9.2.3 All NASA SSPs shall include a System Interconnection Implementation Plan, in accordance with NIST SP 800-47, Appendix C, which describes the purpose and scope of the interconnection implementation plan, including:

a. Certification and accreditation process of the system.

b. Security controls of the system.

c. Recovery and contingency planning for the function.

d. Procedures for reporting and responding to IT security incidents to all participating interconnected systems.

9.3 Additional System Interconnectivity References

NPD 1440.6, NASA Records Management.

Chapter 10 Products and Services

10.1 Acquisition of Products and Services

10.1.1 NASA shall follow the guidance provided in NIST SP 800-35, Guide to IT Security Services, and NIST SP 800-36, Guide to Selecting Information Security Products.

10.1.2 NASA relies heavily on vendor-provided IT products and services, as well as, cooperative agreements and grants. It is critical that NASA incorporate Federal and NASA IT security policies and requirements to safeguard the information and information systems in the acquisition of products and services and the awarding of contracts, grants, and cooperative agreements. Management is required to understand the risk and ramifications associated with the purchasing of products and services and the awarding of contracts, grants, and cooperative agreements.

10.1.3 Once a NASA organization has determined the requirements for a system, it needs to evaluate how to acquire the products and/or services necessary to support that system. NASA can choose to use internal resources including people and existing hardware and software in support of the system or application. However, if these resources do not already exist, NASA management will consider the acquisition of products that have already been evaluated and tested and must understand the full life cycle associated with the acquisition of contracted services in support of that system or application.

10.1.4 NASA management will work with Procurement to develop support service contracts and grants that are flexible enough to ensure that additional IT security requirements are incorporated quickly and efficiently as required by law and by NASA.

10.2 Acquisition Process Requirements

The Procurement Officer and the CIO shall establish procedures to ensure that IT security requirements are incorporated into contracts, grants, and agreements as appropriate. (See Chapter 4, Contracts, Grants, and Agreements)

10.3 Selection of Services Requirements

10.3.1 The selection of IT services shall include:

a. The careful evaluation of options and risks before the selection of resources that will be entrusted to meet NASA's particular IT security program requirements.

b. Consideration of all aspects of the acquisition, implementation, and management of IT services throughout the system's life cycle when they select, implement, or manage IT security services as defined in NIST SP 800-35, Guide to IT Security Services.

c. Services that meet or exceed IT security expectations.

10.4 Selection of Products Requirements

10.4.1 The selection of IT products shall:

a. Consider the threat/risk environment, cost-effectiveness, assurance level, and security functional specifications as appropriate.

b. Ensure that contracts, grants, and agreements address, as a minimum, the security requirements for the purchase of Commercial-Off-The-Shelf (COTS) products, purchase of integrated systems, development of applications, and other IT security-related services. (See Chapter 4, Contracts, Grants, and Agreements.)

c. Acquire products that comply with the NIST FIPS as appropriate.

d. Consider all aspects of the acquisition, implementation, and management of IT products as defined in NIST SP 800-36, Guide to Selecting Information Technology Security Products.

10.5 Additional Products and Services References

a. NIST SP 800-35, Guide to IT Security Services.

b. NIST SP 800-36, Guide to Selecting Information Security Products.

c. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.

Chapter 11 Security Controls

11.1 Controls

11.1.1 Security controls are selected based on the outcome of the analysis of the IT system's security objectives. The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization. Security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system which, when taken together, adequately protect the confidentiality, integrity, and availability of the system and its information.

11.1.2 Given the magnitude of risks inherent in IT operations and the cost associated with IT security controls, all risks can rarely be eliminated. Therefore, a risk management-based approach must be used that finds the right balance between operational needs, limited budgets, identified risks, and available security controls.

11.2 NIST Security Controls

11.2.1 NIST SP 800-53, Recommended Controls for Federal Information Systems, provides a complete catalog of baseline controls based on the impact levels of low, moderate, and high to ensure the confidentiality, integrity, and availability of the system. Based upon the selected IT security category (see Section 7.2, Categorization of Information), specific security controls from NIST SP 800-53 are required to be evaluated against the specific mission and line of business objectives. If the security controls are appropriate for the system, they must be designed into the architecture of the system and system IT security strategy.

11.2.1.1 The baseline set of security controls is the initial starting point. Information system owners must be prepared to increase this set of baseline controls to protect their systems as warranted by their additional requirements or as required by NASA-wide security controls. (See Section 11.3, NASA-wide Common Security Controls.)

11.2.1.2 During the controls selection process, information system owners must continually review their information and information system security strategy. (See Chapter 6, Information and Information System IT Security Strategy.)

11.2.2 NIST Security Controls Requirements

11.2.2.1 All master and subordinate systems shall document, in the Review of Security Controls section of their SSP, the NIST SP 800-53 security controls recommended for the system's IT security category and provide the following information in a Security Controls Assessment Table:

a. NIST control number.

b. Applicability determination (Yes, No, Not Applicable).

c. Control Name.

d. Control Implementation Description.

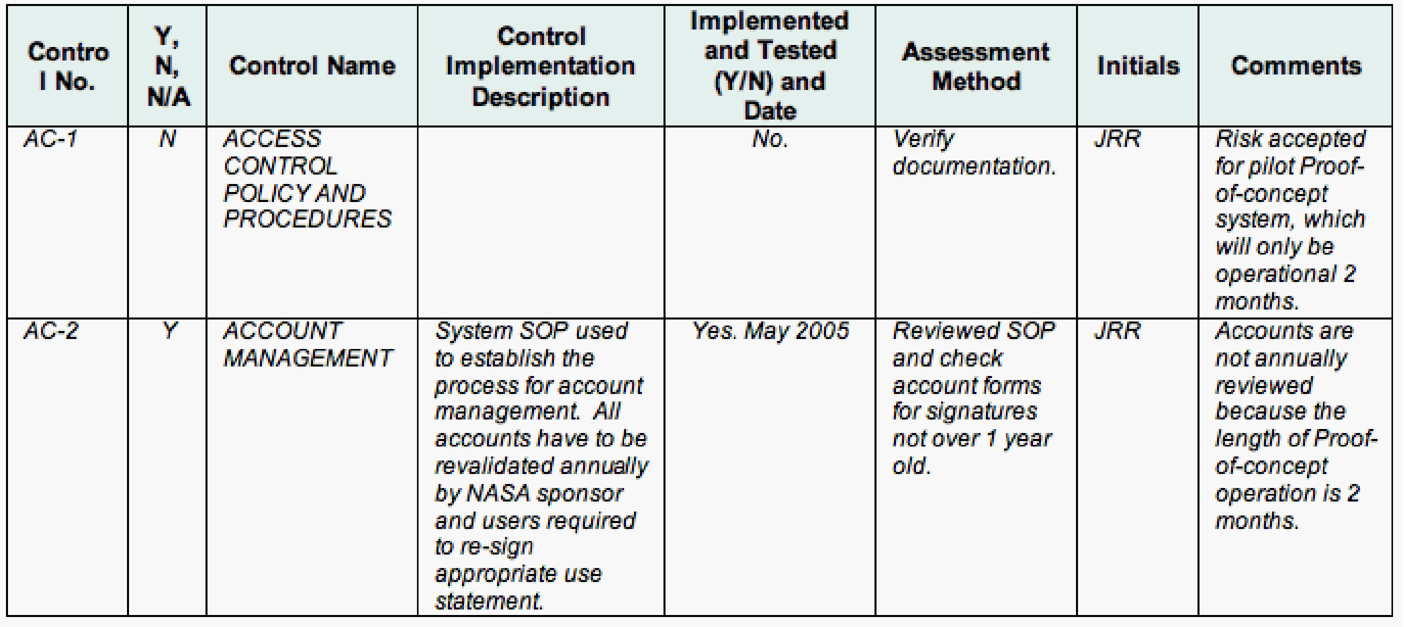
e. Implemented (Yes/No and Date).

f. Assessment Method used to determine that the control was implemented.

g. Initials of individual that determined it was or was not implemented.

h. Comments.

11.2.2.2 The Security Controls Assessment Table shall follow the example format in Figure 11-1. The table can be either in the body of the SSP or included as an appendix to the SSP. The table should present the Control Numbers in the same order as presented in NIST SP 800-53, Recommended Controls for Federal Information Systems, Appendix F.



Control No.	Y, N, N/A	Control Name	Control Implementation Description	Implemented and Tested (Y/N) and Date	Assessment Method	Initials	Comments
AC-1	N	ACCESS CONTROL POLICY AND PROCEDURES		No.	Verify documentation.	JRR	Risk accepted for pilot Proof-of-concept system, which will only be operational 2 months.
AC-2	Y	ACCOUNT MANAGEMENT	System SOP used to establish the process for account management. All accounts have to be revalidated annually by NASA sponsor and users required to re-sign appropriate use statement.	Yes. May 2005	Reviewed SOP and check account forms for signatures not over 1 year old.	JRR	Accounts are not annually reviewed because the length of Proof-of-concept operation is 2 months.

Figure 11-1 Sample Security Controls Assessment Table

11.2.2.3 All security controls determined to be non-applicable to the system shall have the reason for the non-applicability documented in the comments section of the Security Controls Assessment Table and concurred or non-concurred on by the Center ITSM.

11.2.2.4 All security controls that are not implemented, but are applicable to protect the information or the information system, shall be documented as residual risks and tracked in the POA&M for the system.

11.2.2.5 Each control that has not been implemented and has been risk accepted by the AO shall be identified in the comments section of the Security Controls Assessment Table.

11.2.3 NASA-Defined Parameters for NIST Security Controls

11.2.3.1 Some of the security controls in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, Appendix F, Security Control Catalog, provide a degree of flexibility by allowing organizations to define input values for certain parameters associated with the control. This flexibility is achieved using assignment and selection operations within the main body of the control statement. Once specified, the organization-defined value becomes part of the security control, and the organization is assessed against the completed control statement.

11.2.3.2 Responsibility for determining the assignment and selection organizational operational parameters is at the master system level if the controls have not been established as NASA-wide common security controls.

11.2.4 NASA-Defined Parameters for NIST Security Controls Requirements

11.2.4.1 NASA shall define in each master system the optional parameters (i.e., assignment and selection) that will be used by the master system and inherited by its subordinate systems. These parameters will be:

a. Documented in the subordinate system's Security Controls Assessment Table.

b. Verified or tested for implementation during self-assessments of the system.

11.2.4.2 Subordinate systems, for which a master system has not been established, shall assign the security controls parameters, document the selections in the Security Controls Assessment Table of the SSP, and verify or test the security control's implementation during self-assessments of the system.

11.3 NASA-Wide Common Security Controls

11.3.1 NASA has the option to select and enforce certain security controls that shall be adopted by all NASA master and subordinate systems. The NASA SAISO shall publish at least annually a list of those controls that have Agency-wide applicability.

11.3.2 Background Screening of Personnel

11.3.2.1 All personnel granted physical or logical access, including remote logical access, to IT resources not intended for open access by the general public shall undergo background screening and adjudication in accordance with NPR 1600.1, NASA Security Program Procedural Requirements, prior to being granted access and periodically thereafter.

11.3.2.2 Exceptions to the requirements for personnel screening shall be granted by the OSPP in coordination with the OCIO.

11.3.3 Appropriate Use of IT Resources

11.3.3.1 A NASA appropriate use policy statement, based on NPD 2540.1, Personal Use of Government Office Equipment Including IT, and approved by the NASA General Counsel, shall be required from every individual granted access to NASA information systems and networks.

11.3.3.2 The use policy statement in Figure 11-2 shall be the NASA standard.

> Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

Figure 11-2 Appropriate Use Policy Statement

11.3.3.3 Exceptions and modifications to the NASA appropriate use statement to comply with local laws shall be approved by the cognizant NASA General Counsel.

11.3.3.4 The applicable NASA appropriate use policy statement shall be agreed to and acknowledged by either signing the statement or by obtaining an electronic document from the individual acknowledging acceptance of the use policy.

11.3.4 Limited Personal Use of IT Resources

NPD 2540.1, Personal Use of Government Office Equipment, permits NASA employees limited use of IT resources for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. (See NPD 2540.1 for specific uses and restriction.)

11.3.5 Personally-Owned and Company IT Resources

11.3.5.1 Personally-owned IT resources and company-owned resources, utilizing a network IP address, are subject to all network security activities, such as content monitoring, penetration testing, and vulnerability scanning.

11.3.5.2 Personally-owned IT resources and company-owned resources, utilizing a NASA-managed network IP address, shall be approved by the Center NCCB.

11.3.5.3 Personally-owned and company-owned IT resources, utilizing a network IP address, shall comply with NPD 2540.1, Personal Use of Government Office Equipment.

11.3.6 Warning Banners

11.3.6.1 Government computer systems may be targets of hostile activities and subject to other forms of unauthorized use. To counter these activities, the Government may monitor and record the use of Government computer systems through keystroke monitoring and other methods. To deter misuse and notify all users that their use may be monitored, guidance is provided on implementing a warning banner on all appropriate NASA computer systems. This requirement applies to all NASA-owned or NASA-funded IT systems, regardless of location or user, including Government-provided equipment.

11.3.6.2 The NASA General Counsel-approved warning banner shall warn users that their computer, application, and network activities are subject to monitoring, their keystrokes may be monitored and logged, and there is no expectation of privacy. (See Figure 11-3)

> This US Government computer is for authorized users only. By accessing this system you are consenting to complete monitoring with no expectation of privacy. Unauthorized access or use may subject you to disciplinary action and criminal prosecution.

Figure 11-3 NASA-Approved Warning Banner

11.3.6.3 All computers and applications that are owned by or operated on behalf of NASA and requiring user authentication for access shall display and require acknowledgement of the NASA General Counsel-approved warning banner prior to logging on to a NASA system.

11.3.6.4 IT resources not owned by NASA nor operated on behalf of NASA, but utilizing an IP address assigned to NASA, shall be subject to the conditions contained in the NASA warning banner unless a waiver has been granted by the cognizant CIO.

11.3.6.5 Augmentations to the NASA warning banner, to comply with local laws, shall be approved by the NASA or Center Office of the General Counsel.

11.3.6.6 For the current version of the warning banner, see your Center ITSM.

11.3.7 Password Requirements

11.3.7.1 Passwords shall not be electronically transmitted without using encryption.

11.3.7.2 Passwords shall be changed at least annually.

11.3.7.3 Systems shall automatically enforce password attributes, if supported by the system or application.

11.3.7.4 Passwords attributes shall consist of:

a. Between 8 and 128 characters.

b. At least one special character, if supported by the system or application.

c. At least one character from each of the other three character sets: lower-case letters, upper-case letters, and numerals, if supported by the system or application.

11.3.7.5 All vendor-supplied passwords must be identified and changed prior to deployment.

11.3.7.6 Simple Network Management Protocol (SNMP) Community strings and other password-like mechanisms will follow the password requirements.

11.3.7.7 Passwords shall be reset whenever a user forgets a password, when evidence exists that a password may have been compromised, or when management believes that a reset is in the best interest of the security of the system.

11.3.7.8 Passwords attributes shall not consist of:

a. Repeating or consecutive sequence of characters.

b. Information about the user (i.e., username, user ID, office, or function).

c. Dictionary words (i.e., English or other language) even with numerals used to replace letters.

11.3.7.9 Exceptions to the password requirements shall be identified as residual risks and documented in the Accreditation Package presented to the AO.

11.3.8 Computer Support and Operations

11.3.8.1 Computer support and operations include both system administration and tasks external to the system that support its operation, such as maintaining documentation. It does not include system planning or design. The support and operation of any IT system are critical to maintaining the security of a system. Support and operations will include activities that enable IT systems to function correctly. These include fixing software or hardware problems, loading and maintaining software, and helping users resolve problems.

11.3.8.2 The failure to consider security as part of the support and operations of IT systems undermines security measures due to poor documentation, old user accounts, conflicting software, and poor control of maintenance accounts.

11.3.8.3 NASA computer support and operations shall:

a. Ensure that IT support and operations controls are continuously addressed, including hardware maintenance, software maintenance, system and information integrity, and media protection.

b. Implement controls to facilitate system maintenance and to ensure compliance with vulnerability reduction and patch management.

c. Ensure the development and implementation of processes for system access including:

(1) Determining the level of access and privileges a user is given to the information system.

(2) Determining specific processes for access by foreign nationals.

(3) Ensuring that system users and support personnel receive the required security training (e.g., instruction in rules of behavior).

d. Employ antiviral and protection mechanisms to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, removable media, downloaded code, or other methods.

e. Ensure that the computer infrastructure has built-in recovery features (availability), provides adequate baseline protections (confidentiality), and protects data from unauthorized modifications (integrity).

f. Ensure that all NASA systems and data are backed up on a schedule and methodology in accordance with system requirements based on the impact level of the loss of the data.

g. Ensure that mechanisms, in addition to auditing and analysis of audit trails, are implemented to detect unauthorized and illegal acts.

h. Ensure that all ACI or SBU information is categorized in accordance with FIPS 199 and protected in accordance with NIST SP 800-53.

i. Ensure that all required system documentation is:

(1) Maintained and up to date.

(2) Based on the type of system and its category, nature of the information, system software and hardware, applicable laws, FISMA requirements, and requirements for certification and accreditation.

(3) Marked and protected as ACI or SBU where appropriate. (See NPR 1600.1, NASA Security Program Procedural Requirements, for more information).

j. Ensure that all media are labeled with both a description and an appropriate sensitivity marking, such as non-sensitive, or Administratively Controlled Information (ACI), which includes Privacy Act, International Traffic in Arms (ITAR), Export Controlled, Company Proprietary, and information about the security or configuration of NASA IT resources and networks. (See NPR 1600.1).

k. Ensure that all excessed media is properly sanitized following the current NASA memorandum on the Sanitization of NASA Equipment prior to leaving NASA's custody. This can include the destruction of media in a facility rated for the type of information stored on the media.

l. Ensure that the Center/Mission Directorate network and IT security system support and operations staffs have the skills and resources necessary to identify security problems, respond appropriately, inform appropriate individuals, and assist users.

m. Ensure that there is a separation of duties for critical operations.

11.3.9 Internet Publishing Content Requirements

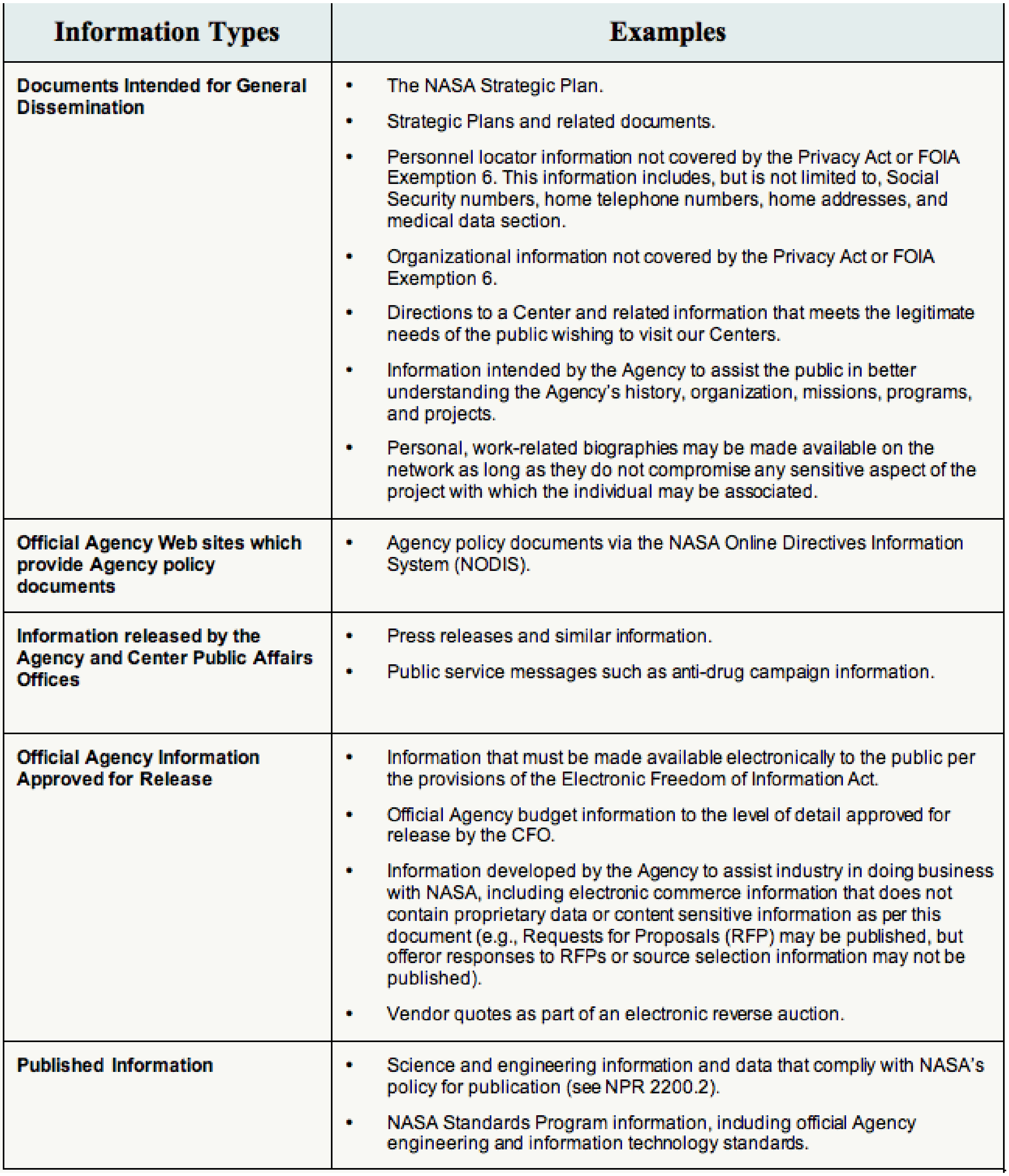
11.3.9.1 Publication via the Internet is defined as making information available to the public-at-large via the Transport Control Protocol/Internet Protocol (TCP/IP) network protocol without authentication. This includes, but is not limited to, hypertext transfer protocol HTTP (hypertext transfer protocol), associated protocols (i.e., World Wide Web), and anonymous File Transfer Protocol (FTP) traffic, as well as any other application (e.g., bulletin boards or chart groups) that makes NASA information accessible to the public at large via IP.

11.3.9.2 NASA management and NASA personnel shall:

a. Comply with existing laws and policies that restrict the distribution of information.

b. Understand that all NASA information and data available to the public at large via the Internet, unless protected by appropriate access controls, are considered published and subject to the requirements of this document and references identified below.

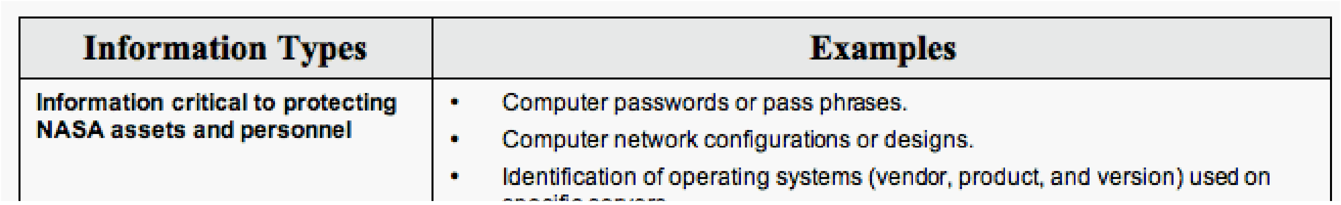
11.3.9.3 All documents planned to be made available on the network shall be analyzed before publication against the guidelines listed in Figure 11-4 to ensure that they do not contain information that is inappropriate for public dissemination. Figure 11-4 is not all-inclusive, but is intended to provide examples of information that may be appropriate for publication.



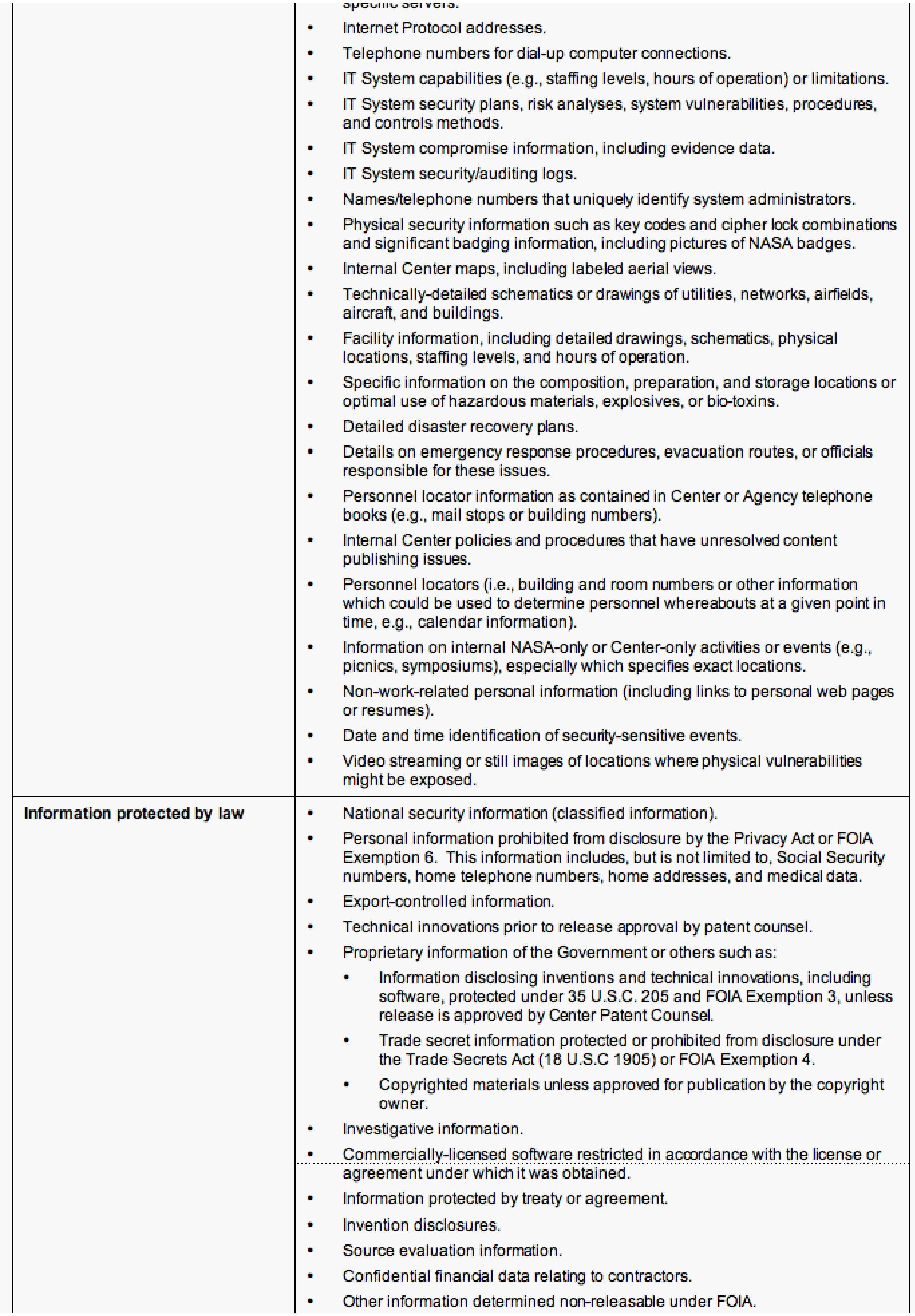
Information Types	Examples
Documents Intended for General Dissemination	• The NASA Strategic Plan. • Strategic Plans and related documents. • Personnel locator information not covered by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data section. • Organizational information not covered by the Privacy Act or FOIA Exemption 6. • Directions to a Center and related information that meets the legitimate needs of the public wishing to visit our Centers. • Information intended by the Agency to assist the public in better understanding the Agency's history, organization, missions, programs, and projects. • Personal, work-related biographies may be made available on the network as long as they do not compromise any sensitive aspect of the project with which the individual may be associated.
Official Agency Web sites which provide Agency policy documents	• Agency policy documents via the NASA Online Directives Information System (NODIS).
Information released by the Agency and Center Public Affairs Offices	• Press releases and similar information. • Public service messages such as anti-drug campaign information.
Official Agency Information Approved for Release	• Information that must be made available electronically to the public per the provisions of the Electronic Freedom of Information Act. • Official Agency budget information to the level of detail approved for release by the CFO. • Information developed by the Agency to assist industry in doing business with NASA, including electronic commerce information that does not contain proprietary data or content sensitive information as per this document (e.g., Requests for Proposals (RFP) may be published, but offeror responses to RFPs or source selection information may not be published). • Vendor quotes as part of an electronic reverse auction.
Published Information	• Science and engineering information and data that comply with NASA's policy for publication (see NPR 2200.2). • NASA Standards Program information, including official Agency engineering and information technology standards.

Figure 11-4 Information Appropriate for Publication on the Internet

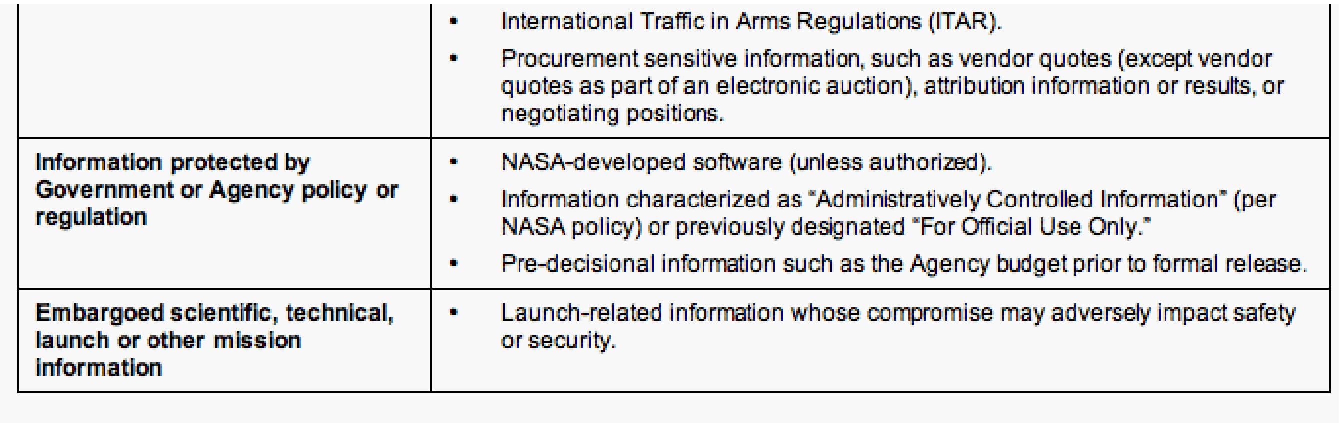
11.3.9.4 The following information shall not be made available to the public at large via the Internet. If this information is made available via the Internet, security mechanisms shall be implemented to ensure that the information is available only to its intended, limited audience. Figure 11-5 is not all-inclusive but is intended to provide examples of information inappropriate for publication.



Information Types	Examples
Information critical to protecting NASA assets and personnel	• Computer passwords or pass phrases. • Computer network configurations or designs. • Identification of operating systems (vendor, product, and version) used on



	specific servers. • Internet Protocol addresses. • Telephone numbers for dial-up computer connections. • IT System capabilities (e.g., staffing levels, hours of operation) or limitations. • IT System security plans, risk analyses, system vulnerabilities, procedures, and controls methods. • IT System compromise information, including evidence data. • IT System security/auditing logs. • Names/telephone numbers that uniquely identify system administrators. • Physical security information such as key codes and cipher lock combinations and significant badging information, including pictures of NASA badges. • Internal Center maps, including labeled aerial views. • Technically-detailed schematics or drawings of utilities, networks, airfields, aircraft, and buildings. • Facility information, including detailed drawings, schematics, physical locations, staffing levels, and hours of operation. • Specific information on the composition, preparation, and storage locations or optimal use of hazardous materials, explosives, or bio-toxins. • Detailed disaster recovery plans. • Details on emergency response procedures, evacuation routes, or officials responsible for these issues. • Personnel locator information as contained in Center or Agency telephone books (e.g., mail stops or building numbers). • Internal Center policies and procedures that have unresolved content publishing issues. • Personnel locators (i.e., building and room numbers or other information which could be used to determine personnel whereabouts at a given point in time, e.g., calendar information). • Information on internal NASA-only or Center-only activities or events (e.g., picnics, symposiums), especially which specifies exact locations. • Non-work-related personal information (including links to personal web pages or resumes). • Date and time identification of security-sensitive events. • Video streaming or still images of locations where physical vulnerabilities might be exposed.
Information protected by law	• National security information (classified information). • Personal information prohibited from disclosure by the Privacy Act or FOIA Exemption 6. This information includes, but is not limited to, Social Security numbers, home telephone numbers, home addresses, and medical data. • Export-controlled information. • Technical innovations prior to release approval by patent counsel. • Proprietary information of the Government or others such as: • Information disclosing inventions and technical innovations, including software, protected under 35 U.S.C. 205 and FOIA Exemption 3, unless release is approved by Center Patent Counsel. • Trade secret information protected or prohibited from disclosure under the Trade Secrets Act (18 U.S.C 1905) or FOIA Exemption 4. • Copyrighted materials unless approved for publication by the copyright owner. • Investigative information. • Commercially-licensed software restricted in accordance with the license or agreement under which it was obtained. • Information protected by treaty or agreement. • Invention disclosures. • Source evaluation information. • Confidential financial data relating to contractors. • Other information determined non-releasable under FOIA.



	• International Traffic in Arms Regulations (ITAR). • Procurement sensitive information, such as vendor quotes (except vendor quotes as part of an electronic auction), attribution information or results, or negotiating positions.
Information protected by Government or Agency policy or regulation	• NASA-developed software (unless authorized). • Information characterized as "Administratively Controlled Information" (per NASA policy) or previously designated "For Official Use Only." • Pre-decisional information such as the Agency budget prior to formal release.
Embargoed scientific, technical, launch or other mission information	• Launch-related information whose compromise may adversely impact safety or security.

Figure 11-5 Information Not Appropriate for Publication on the Internet

11.3.10 Use of Wireless Local Area Networks

11.3.10.1 The use of wireless local area networks (WLANS) provides wider capability to access the wired network through mobile computing devices. However, with the added benefits of wireless networking also comes additional risk. If implemented without the appropriate security controls, a wireless network can easily be exploited and used as a conduit for unauthorized network access, misuse, and abuse. Those responsible for the installation and operation of a wireless network must be aware of the inherent risks that exist in a wireless environment and its impact on a Center's Information Technology (IT) security posture.

11.3.10.2 Wireless Requirements

11.3.10.2.1 Wireless IT resources shall be designed and implemented to protect the confidentially, integrity, and availability of NASA's information.

11.3.10.2.2 All WLANs and wireless access points shall be approved by the Center NCCB and treated as part of the network infrastructure following all existing security and network standards, policies, and procedures. Adhoc networks are prohibited.

11.3.10.2.3 WLANs shall be monitored by the Center CIO.

11.3.10.2.4 All WLANs and wireless access points, architecture designs, and implementation shall follow NASA ITS-SOP-0020, Wireless Local Area Network Security Procedures.

11.3.10.2.5 Waivers for special circumstances shall be submitted for consideration to the Center NCCB and approved or disapproved by the Center CIO on a case-by-case basis. A security assessment and impact report shall be required for all waivers and documented in the appropriate SSP.

11.3.10.2.6 A full Center site survey shall be performed at least semi-annually to detect unauthorized WLAN access points. Spot checks for unauthorized WLAN access points shall be performed quarterly.

11.3.11 Peer-to-Peer (P2P) Connections

11.3.11.1 NASA shall follow OMB, Memorandum for CIOs' ; dated September 8, 2004; subject: Personal Use Policy and "File Sharing" Technology, which provides direction for establishing NASA P2P requirements.

11.3.11.2 Unapproved P2P file sharing technology has inherent security risks of downloading information from sites which may contain programs that pose considerable risks to NASA's IT infrastructure by introducing viruses, worms, Trojan horses, and other malicious code. Installing P2P software can make the system more vulnerable to compromises and unintended sharing of information from its hard drive. Federal law is clear and explicitly forbids the illegal distribution or other inappropriate use of copyrighted material.

11.3.12 P2P Requirements

11.3.12.1 Centers should actively prevent the use of unauthorized P2P file sharing.

11.3.12.2 The Center NCCBs shall implement port blocking and/or bandwidth/rate limiting to block or limit the most frequently used Internet ports for P2P file sharing applications. (Contact the Center ITSM for the most recent list of P2P ports.)

11.3.12.3 P2P file sharing technology shall only be utilized when approved, case-by-case, by the Center CIO or CIO designee and documented with the appropriate NCCB.

11.3.12.4 Unauthorized P2P traffic, once identified and traced back to a user by the Center ITSM, shall be blocked and the appropriate management notified to take appropriate administrative actions for the policy violation.

11.3.3 Network Security

11.3.13.1 Networks allow systems to connect for the sharing of data and files, as well as providing access to the resources themselves. The security architecture and configuration control of a network permits network connected systems to interact securely without jeopardizing their own security controls. Typically within NASA, there are WANs, LANs, WLANs, project-level networks, and network address translation (NAT) networks with private address space.

11.3.13.2 Each network is established to provide a different level of protection and typically connected in a layered fashion from the WAN to LAN to project level or NAT networks. Most NASA systems have a connection to a public network such as the Internet which is considered non-secure and presents threats that must be countered by security controls, vigilance, and monitoring. NASA systems that connect to networks operated by others shall review and concur on the protective measures and risk inherent in connecting to the network.

11.3.13.3 Network Security Requirements

11.3.13.4 All network architectures shall follow the NASA Enterprise Architecture which includes: border routers, firewalls, virtual private networks (VPNs), intrusion detection systems (IDS), and other associated network infrastructure. Guidance can be found in:

a. NIST SP 800-31, Intrusion Detection Systems.

b. NIST SP 800-41, Guides on Firewalls and Firewall Policy.

c. NIST SP 800-44, Guidelines on Securing Public Web Servers.

d. NIST SP 800-45, Guidelines on Electronic Mail Security.

e. NIST SP 800-46, Telecommuting and Broadband Communications.

f. NIST SP 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices.

g. NIST SP 800-58, Security Considerations for Voice Over IP Systems.

h. NIST SP 800-77, Guide to IP Sec VPNs.

11.3.13.5 All NASA networks, including wireless networks, shall:

a. Be either part of a subordinate SSP or be a subordinate system under the OAIT master system for networking.

b. Describe their security controls in their SSP and identify in the Risk Assessment Summary any residual risks that are to be accepted by the AO.

c. Be managed in accordance with NASA's SOPs on network and wireless network security.

11.3.13.6 Networks operated and managed under contracts, cooperative agreements, grants, partnership agreements, agreements with international partners, university partners and other educational entities, NASA Space Act Agreements, and special volunteer partners shall establish configuration control of their networks, document modifications to the approved configurations, and notify their customers of changes to the security controls.

11.3.13.7 All network operations shall document all approved network devices making up the network and connected systems and monitor for unapproved devices and systems.

11.3.13.8 Remote connection to NASA networks from an Internet Service Provider (ISP) shall require encrypted authentication and data transmission, such as by a Virtual Private Network (VPN).

11.3.13.9 Remote privileged access to a NASA system from outside NASA network space shall require two-factor authentication and encrypted data transmission.

11.3.13.10 Each Center shall have a NCCB that shall:

a. Conduct a risk assessment for modifications to the network.

b. Approve or disapprove all proposed modifications.

c. Provide notification to its customers of all modifications that would affect the protections provided by the network.

d. Document all Center NCCB actions and, if appropriate, ensure that the affected SSPs are updated and the AO notified for possible recertification and reaccreditation prior to the modification being implemented.

e. Have the authority to disconnect or deny service to any network-attached device, including wireless devices, in the event of an incident or violation of the rules of the systems or acceptable use policy.

11.3.4 Penetration Testing

11.3.4.1 A security penetration test is an activity in which a test team attempts to circumvent the security processes and controls of a computer system to include social engineering. Posing as either internal or external unauthorized intruders, the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the target computer in unauthorized ways. Due to the sensitive nature of the testing, specific rules of engagement are necessary to ensure that testing is performed in a manner that minimizes impact on operations while maximizing the usefulness of the test results.

11.3.4.2 Penetration Testing Requirements

11.3.4.3 NASA shall ensure that penetration testing is conducted only in conjunction with the Center CIO, the Center ITSM, the affected system administrator's network operation, and IT security staff and will be performed in a spirit of a joint training exercise by all participants.

11.3.4.4 Penetration testing shall follow ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting.

11.3.4.5 The OCIO or cognizant Center CIO shall approve all penetration testing run against NASA IP address space.

11.3.4.6 Results from penetration testing shall be considered ACI or SBU information and will be handled and protected accordingly.

11.3.4.7 Rules of engagement must be agreed to, documented, and signed by all parties prior to the initiation of penetration testing following ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting.

11.3.4.8 A non-disclosure agreement shall be signed by a non-NASA reviewer.

11.3.5 System and Communication Protection Requirements

11.3.5.1 For unclassified IT resources, NASA shall comply with National policy by ensuring that all valuable information and information systems are afforded an adequate degree of protection that is commensurate with the risks posed to NASA IT resources and the magnitude of potential harm that could be experienced by NASA if IT resources are compromised or sensitive information is inadvertently disclosed. To achieve this goal, NASA has established standards for encryption and digital signatures in NASA STD 2820, Encryption and Digital Signature Standards. NASA management shall comply with NIST FIPS Publication 140-2, Security Requirements for Cryptographic Modules, FIPS Publication 46-3, Data Encryption Standard and NIST SP 800-77, Guide to IPSec VPNs. Specific NASA requirements follow.

11.3.5.2 Only National Security Agency (NSA) approved and endorsed encryption products and/or techniques shall be used for protecting all telemetry and telecommunications involving:

a. Radio transmissions or signals for command/destruct uplinks to launch vehicles, spacecraft, test aircraft, and other manned or unmanned aerospace vehicles.

b. Commanding of command and control links to vehicles for vehicle housekeeping activities.

c. Payload operations including command and control of the payload and the handling of raw data from spacecraft payloads.

11.3.5.3 The encryption level, strength, and type shall be based upon risk and cost assessments conducted by the program or project management and will be NSA and/or NIST-approved and endorsed encryption products and/or techniques.

11.3.5.4 All NASA PCAs shall address the requirement for data encryption and document the decision and the determination of the type, level, and strength of the encryption that will be used.

11.3.5.5 All command/destruct uplinks to launch vehicles, spacecraft, test aircraft, and other manned or unmanned aerospace vehicles shall utilize NSA and/or NIST-approved or endorsed techniques and products. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and submitted to the OSPP with concurrence by the OCIO.

11.3.5.6 All command and control links to vehicles for vehicle housekeeping activities shall:

a. Utilize NSA and/or NIST-approved or endorsed techniques and products.

b. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and shall be submitted to the OSPP for approval with concurrence by the OCIO.

11.3.5.7 All payload operations including command and control of the payload and the handling of raw data from spacecraft payloads shall:

a. Utilize NSA and/or NIST-approved or endorsed techniques and products.

b. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and shall be submitted to the OSPP for approval with concurrence by the OCIO.

11.3.5.8 NASA systems and applications whose information security category is rated high or moderate (see Chapter 7, System Characterization, Information Categorization, System Types, and System Boundaries) shall:

a. Be evaluated for the impact of not utilizing encryption as a security control by considering not only the value of information and the cost of recovery, but also the intangible costs of possible harm or loss, which may equal or outweigh, the measurable costs.

b. Document the decision to use or not to use encryption in the SSP.

c. If the decision is to use encryption, utilize NSA and/or NIST-approved or endorsed techniques and products.

11.3.5.9 ACI or SBU information, as determined by NPR 1600.1, NASA Security Program Procedural Requirements, shall be encrypted in transmission and shall:

a. Utilize NSA and/or NIST-approved or endorsed techniques and products.

b. Waivers/variances/exceptions to the requirement to use NSA and/or NIST products shall be considered on a case-by-case basis and shall be submitted to the OSPP for approval with concurrence by the OCIO.

11.4 Additional Security Controls References

a. NPR 1441.1, Records Retention Schedule.

b. NPD 1382.17, Privacy Act - Internal NASA Direction in Furtherance of NASA Regulations.

c. NPD 1600.2 NASA Security Program Policy.

d. NPR 1600.6 Communications Security Procedures and Guidelines.

e. NPR 1620.1, Security Procedures and Guidelines.

f. NPD 2110.1, Foreign Access to NASA Technology Transfer Materials.

g. NPD 2190.1, NASA Export Control Program.

h. NPR 2200.2, Guidelines for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information.

i. NPR 2210.1, External Release of NASA Software.

j. NPD 2220.5, Management of NASA Scientific and Technical Information (STI).

k. NPR 2800.1, Managing Information Technology.

l. NPD 2810.1, NASA Information Security.

m. NPD 2820.1, NASA Software Policy.

n. NPD 7120.4, Program/Project Management.

o. NPR 7120.5, NASA Program and Project Management Processes and Requirements.

p. NPR 7150.2, Software Engineering Requirements.

q. NASA Technical Standards, Series 2800, Computer Systems, Software, Information Systems.

r. NASA's E-FOIA Regulations, 64 Federal Register 39,401-39,414 (1999) (codified at 14 CFR Part 1206).

s. NIST SP 800-12, Introduction to Computer Security: The NIST Handbook: Computer Support and Operations Requirements.

t. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.

u. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems.

v. NIST SP 800-27, Engineering Principles for IT Security.

w. NIST SP 800-28, Guidelines on Active Content and Mobile Code.

x. NIST SP 800-31, Intrusion Detection Systems.

y. NIST SP 800-41, Guides on Firewalls and Firewall Policy.

x. NIST SP 800-42, Guidelines on Network Security Testing.

aa. NIST SP 800-44, Guidelines on Securing Public Web Servers.

ab. NIST SP 800-45, Guidelines on Electronic Mail Security.

ac. NIST SP 800-46, Telecommuting and Broadband Communications.

ad. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.

ae. NIST SP 800-48, Wireless Network Security 802.11, Bluetooth and Handheld Devices.

af. NIST SP 800-77, Guide to IP Sec VPNs.

ag. Attorney General Policy Memorandum of October 12, 2001 on the Freedom of Information Act, Appropriate Account and Use of IT Resources.

SECTION III MANAGEMENT CONTROLS

Chapter 12 IT Security Risk Management

12.1 IT Security Risk Management Overview

12.1.1 NASA shall follow the NPR 8000.4, Risk Management Procedural Requirements, and include the requirements of NIST SP 800-30, Risk Management Guide for Information Technology System, for guidance on risk management processes. This chapter provides a high-level summary of risk management.

12.1.2 NASA accepts that complete avoidance of IT security risk is not cost-effective and may impact mission success. NASA management will ensure that IT security risks are assessed, analyzed, and mitigated to the point that residual risks are considered acceptable by management. Implicit to this concept is a "tailored" approach to IT security protection, in which information and functions of differing criticality are protected at different levels.

12.1.3 The IT security risk management program encompasses three processes: risk assessment, risk mitigation, and continuous risk management. These processes are continued throughout the system's life cycle from initiation to disposal and are performed at varying levels of complexity as the system matures.

12.2 Risk Management Process Requirements

12.2.1 The IT security risk management process shall:

a. Treat the NASA IT risk management process as an essential management function and not as a technical function primarily carried out by the IT experts who operate and manage the IT system.

b. Ensure that system risk analyses, risk mitigation alternatives analyses, and building a business case for the acquisition of appropriate security are coordinated and performed.

c. Ensure that all activities in the NASA risk management process address IT security for all information systems and applications.

d. Ensure that appropriate security is implemented to protect the system's information, including the implementation and maintenance of management, operational, and technical controls by working closely with system support personnel.

e. Define the potential impact on projects should a breach in security occur (i.e., a loss of confidentiality, integrity, or availability). Ensure that the system and information owners concur on the risks in accordance with NIST SP 800-30, which states "regardless of the method used to determine how sensitive an IT system and its data are, the System and Information Owners are the ones responsible for determining the impact level for their own system and information."

f. Determine the impact of security threats to the security objectives and then identify the proper measures that are required to protect against the unwanted disclosure of information, inadvertent or malicious corruption of data, or denial of authorized access to the system.

g. Balance both the operational and economic costs of measures to protect the IT systems and the information that support NASA missions. Assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

h. Ensure that all IT security risk management activities are performed whenever there is a significant change to the system or whenever a new risk is identified that will impact the current security posture.

i. Implement policies and procedures to cost-effectively manage risks to an acceptable impact level.

j. Annually test and evaluate a subset of information security controls and techniques to ensure that they are effectively implemented. Information system owners may define a subset of high impact controls to test annually. Further, the SAISO may publish a list of controls to be tested annually through a Directive letter.

k. Ensure that test results and resulting IT security recommendations are adopted as appropriate and that the choices are fully documented in the corresponding SSP.

l. Ensure that any unmitigated risks are documented in a POA&M.

12.2.2 Risk Assessment Process Requirements

12.2.2.1 NASA shall use NIST SP 800-30, Risk Management Guide for Information Technology System, Appendix B, Sample Risk Assessment Report Outline, which shall be summarized in the SSP and attached as an appendix to the SSP.

12.2.2.2 NASA shall use NIST SP 800-30, Risk Management Guide for Information Technology System, Appendix C, Sample Safeguard Implementation Plan Summary Table, which shall be attached as an appendix to the SSP.

12.2.2.3 Risk assessments shall be conducted based on system characterization as described in section 7.2, Categorization of Information.

12.2.2.4 The IT security risk assessment process shall:

a. Ensure that IT security risk assessment is an ongoing process and is conducted and integrated in the SDLC for all NASA IT systems and information resources.

b. Ensure that periodic assessments are performed throughout the SDLC of their information systems to determine the risk and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Agency

c. Determine the appropriate levels of information security as described in section 7.2, Categorization of Information.

d. Ensure that a preliminary risk assessment is conducted for all information systems and applications, prior to system procurement, to estimate the level of impact associated with the planned information system.

e. Ensure that risk assessments and analyses for Agency master and subordinate IT Systems are conducted. Conduct risk assessments for subordinate IT systems based upon NIST's list of management controls, operational controls, and technical controls for the security category of the information system and any inherited controls from the master IT System. Focus of the risk assessment for the subordinate system will be on site-specific threats and vulnerabilities.

f. Ensure that a risk assessment summary report describing the information's security category and detailing the vulnerability/threat pairs, risk assessment results, and the potential impact is presented to the AO as part of the Certification and Accreditation Package.

g. Ensure that a IT security risk assessment team is assigned to facilitate and assist in analytical duties for risk assessment activities.

12.2.3 Risk Mitigation Process Requirements

12.2.3.1 NASA risk mitigation process shall:

a. Employ systematic methodologies to mitigate system IT security risk.

b. Prioritize, evaluate, and implement the appropriate cost-effective, risk-reducing controls recommended from the risk assessment process.

c. Ensure that test results and the resulting IT security recommendations are adopted as appropriate and that the choices are fully documented in the corresponding SSP.

d. Provide a record showing that the security controls were verified or tested, who verified or tested the controls, and if the verification or testing results were acceptable or unacceptable.

e. Provide the justification for any security controls that are not appropriate for the system in the Security Controls Assessment Table.

12.2.4 NASA Continuous Risk Management Process

12.2.4.1 NASA shall employ continuous a risk management process to:

a. Ensure that programs and projects integrate IT security risk management as defined in NIST SP 800-30, Risk Management Guide for Information Technology System, with the processes and procedures defined in NPR 7120.5, NASA Program and Project Management Process and Requirements, and NPR 8000.4, Risk Management Procedural Requirements.

b. Ensure that IT security risk assessment is an ongoing process and that risk management is conducted and integrated in the SDLC for all NASA IT systems and information resources in support of the NASA missions.

12.3 Additional IT Security Risk Management References

a. NIST SP 800-30, Risk Management Guide for Information Technology System.

b. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information.

c. NPR 7120.5, NASA Program and Project Management Processes and Requirements.

d. NPR 8000.4, Risk Management Procedural Requirements.

Chapter 13 IT System Security Planning

13.1 IT System Security Planning Overview

13.1.1 NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, provides the bulk of the guidance for preparing NASA's IT SSPs. NASA provides ITS-SOP-0016, Information Technology SSP, which fills in the gaps in the NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems that were caused by subsequent NIST publications.

13.1.2 All IT systems support NASA's enterprise architecture.

13.1.3 The purpose of an IT SSP is to:

a. Provide an overview of the system security requirements and pertinent risks and describe the controls that are planned for, or are already in place, that will result in cost-effective risk management and protection for the system and associated information.

b. Delineate the responsibilities and the expected behavior of all individuals who access the system or the information contained in the system.

c. Document the results of the security control selection and specification process, including justification and rationale for the final security controls selected and how the controls meet NASA's IT security requirements.

d. Provide the information system owner, the CA, and the AO the information necessary to make informed risk management decisions.

e. Contain requirements for various managers with responsibilities concerning the system, including information owners, the system administrator, and the system security manager.

13.1.4 The SSP is a critical document required as input for the security certification process that demonstrates that the controls designed and implemented for the system are adequate to protect NASA's information. Once the system has been certified, a NASA management official shall accredit the system prior to its going operational. The accrediting NASA AO assumes the risk of the system going operational and shall ensure that all controls have been validated by the CA. The accreditation of a system to process information provides an important quality control. (See Chapter 14, System Certification and Accreditation.)

13.1.5 IT SSPs will be grouped according to the guidance provided by the NASA SAISO, which can be found in Chapter 8, Master and IT Subordinate Systems.

13.2 IT System Security Plan Requirements

13.2.1 All master and subordinate system plans shall be developed using the ITS-SOP-0016, Information Technology SSP, for developing their SSPs. Since the SSP is a living document, sections shall be added to the plan or modified as the system matures.

13.2.2 The complete SSP, as developed and maintained by the information system owner, shall include:

a. SSP Executive Summary.

b. Document revision log.

c. Letter of accreditation.

d. Statement of Readiness for C&A.

e. Body of the SSP.

f. Attachments including, but not limited to, the acronym list, risk assessment documentation, contingency plan, interconnectivity agreements, POA&M, and other required documentation not included in the body of the SSP.

g. For MEI systems, a brief description of the rationale used for categorizing the system as an MEI along with the date that the OSPP approved the MEI determination.

13.2.3 All SSPs shall be protected as ACI or SBU information.

13.2.4 The SSP must be developed and reviewed for completeness prior to proceeding with the certification and accreditation process. Information system owners shall provide an acknowledgement statement that:

a. Indicates that the signers have reviewed the SSP and that it accurately reflects the system design, IT security strategy, the information's security category, risks that were accepted, and that the POA&M reflects the status of the tasks that need to be accomplished to obtain full ATO.

b. Provides for the concurrence/non-concurrence signatures of the information system owner, information owners, lead CA, and SSP preparers.

c. Provides for the endorsement by the appropriate CIO, ITSM, and OSPP representative to proceed with the C&A process.

13.2.5 The SSP POA&M shall:

a. Identify tasks that must be accomplished prior to the system's being granted a full ATO.

b. Identify the resources required to accomplish each task.

c. Identify the milestones to be tracked in meeting the task.

d. Identify a schedule completion date for each milestone and task.

13.2.6 The Contingency Plan shall:

a. Summarize the requirements for continuity of critical operational processes and identify the individual responsible for the development and maintenance of the contingency plan.

b. See Chapter 15, System Contingency Planning, for complete guidance on contingency planning.

13.3 Additional IT System Security Plan References

a. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems.

b. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

c. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

Chapter 14 - System Certification and Accreditation

14.1 Certification and Accreditation

14.1.1 NASA shall follow NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, guidance in performing certification and accreditation.

14.1.2 NASA shall use ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment.

14.1.3 The C&A process is a mandatory FISMA process used to ensure that IT systems have effective security controls that have been implemented, or planned for, commensurate with the potential risks to the information. This process is applicable throughout the system's life cycle, including those systems under development and those already in production.

14.1.4 Certification and accreditation activities shall be performed at least once every three years or following a major change to the system.

14.1.5 The C&A process has four distinct phases: initiation, certification, accreditation, and continuous monitoring. Each of these phases is addressed in every IT system accreditation for both operational systems and systems under development regardless of where the system is in the life cycle process.

14.2 Certification Process

Certification is the comprehensive assessment of the technical and non-technical security features and other safeguards of an IT system and establishes the extent to which a particular design and implementation meets documented security requirements. The certification team, led by a CA, can be an individual, group, or organization.

14.3 Certification Process Requirements

14.3.1 The certification and accreditation process shall apply to all master and subordinate systems.

14.3.2 The certification agent shall:

a. Be responsible for conducting a security certification to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the system's security requirements.

b. Provide the information system owner during the initiation phase with an independent assessment of the SSP to ensure that the plan has documented a set of security controls that is adequate to meet all applicable security requirements.

c. Provide findings and recommendations to the information system owner, who can take corrective actions and update the SSP.

d Document the unmitigated risks in a security assessment report after corrective actions have been made by the information system owner.

14.3.3 Certification of systems that are categorized at the low security impact level shall:

a. Have a "self assessment" of the security controls conducted by the information system owner utilizing ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment. The security assessment report shall be reviewed by the Center ITSM and included in the SSP by the information system owner.

b. Result in the development of an Accreditation Package as prepared by the CA (see Section 2.5.3.3 e) including:

(1) A transmittal letter. See NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Appendix E, for a sample transmittal letter.

(2) A copy of the approved SSP.

(3) The POA&M.

c. Deliver the Accreditation Package to the cognizant Center CIO, ITSM, and the AO as required.

14.3.4 The certification of systems that are categorized at the high or moderate security impact level shall:

a. Consist of a "self assessment" of the security controls conducted by the information system owner utilizing NASA ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment, until the NIST SP 800-26 and the Agency independent third-party, approved by OSPP, performs the certification of the system. The self-assessment is performed prior to tasking with the independent certifier. The security assessment report shall be reviewed by the Center ITSM and included in the SSP by the information system owner.

(1) Between the initiation phase and the certification phase, information system owners of IT systems that require Agency contractor certification shall request that the OSPP conduct a review and spot check to ensure security controls are documented during the preparation phase.

(2) Once the OSPP review is satisfactorily completed, the Agency-approved third party, can initiate the certification phase, which constitutes an independent audit.

b. Result in the development an Accreditation Package including:

(1) A transmittal letter; See NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Appendix E, for a sample transmittal letter.

(2) Copy of the approved SSP.

(3) The POA&M.

c. Deliver the Accreditation Package to the cognizant Center CIO, ITSM, and the AO as required.

14.3.5 The information system owner shall be responsible for preparing or updating an existing POA&M documenting the remaining actions needed to meet the security requirements of the system.

14.3.6 All SSP packages, in order to prepare for future recertification, shall include a C&A change log to document:

a. Changes made to the system or its environment.

b. In a Security Impact Analysis report, any impact the change may have on the system.

c. Steps taken to eliminate or mitigate any risks resulting from the change.

d. The impact upon the security accreditation decision.

14.4 Accreditation Process

14.4.1 Accreditation is the formal declaration by an AO that an IT system is compliant with established security requirements and is approved to operate using a prescribed set of safeguards. This decision should be based on the residual risks identified during the risk mitigation process. By accrediting an information system, the AO accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

14.4.2 The security accreditation package documents the results of the security certification process and provides the AO with the essential information needed to make a credible, risk-based decision on whether or not to authorize operation of the information system. The responsibility of the AO for the security accreditation decision and the signing of the accreditation letter (i.e., the acceptability of risk to NASA) cannot be delegated. The information system owner is responsible for the assembly, compilation, and submission of the security accreditation package.

14.4.3 The accreditation phase consists of the security accreditation decision and the security accreditation documentation. The AO shall make one of three decisions:

a. Full Authorization to Operate is issued for the information system if, after assessing the results of the security certification, the residual risk to NASA's operations or assets is deemed fully acceptable to the NASA AO. The information system is accredited without any significant restrictions or limitations on its operation.

b. Interim Authorization to Operate (IATO) is issued if, after assessing the results of the security certification, the residual risk to NASA's operations or assets is not deemed fully acceptable to the NASA AO, and there is an overarching need to place the information system into operation or continue its operation due to mission necessity. An interim authorization provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to NASA's operations and assets for a limited period. The information system is not considered accredited during the period of IATO. The IATO will not exceed six months.

c. Denial of Authorization to Operate is issued if, after assessing the results of the security certification, the residual risk to NASA's operations or assets is deemed unacceptable to the NASA AO. The information system is not accredited and will not be placed into operation. For an information system currently in operation, all activity will be halted. Failure to receive ATO or an IATO usually indicates that there are major deficiencies in the security controls of the information system. The NASA AO shall work with the information system owner to revise the POA&M to ensure that proactive measures are taken to correct the security deficiencies.

14.4.4 NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Section 3.3, details the process and documentation requirements NASA shall follow for accomplishing the security accreditation process and Section 14.5, Accreditation Process Requirements, below, adds specific NASA requirements.

14.5 Accreditation Process Requirements

14.5.1 Responsibility for the security accreditation decision shall not be delegated. Those authorized to act in a functional position in the primary's absence shall inherit the AO's responsibilities. The AO's role shall be consistent with NPD 1000.3, The NASA Organization. The current role of AOs for master and subordinate systems is documented in Figure 14-1.

If the System is,	Then the Master System Authorizing Official is the	And the Subordinate System Authorizing Official is the
Office Automation of Information Technology (OAIT)	NASA Deputy CIO	Center CIO
Program Unique	Deputy Associate Administrator for the Mission Directorate funding the system	Deputy Associate Administrator for the Mission Directorate funding the system

A Multi-funded system (majority funded by single Mission Directorate)	Deputy Associate Administrator for the Mission Directorate funding the majority of the system	Deputy Associate Administrator for the Mission Directorate funding the majority of the system
A Multi-funded system (no majority Mission Directorate funding)	Appropriate Deputy Center Director Directorate	Deputy Center Director
Institutions and Management's Responsibility	Deputy Assistant Administrator for the Appropriate Functional Area	Center CIO
For the Office of Inspector General	NASA Deputy OIG	NASA Deputy OIG
For Office of Safety and Mission Assurance	Deputy Chief Safety and Mission Assurance Officer	Center CIO
For the Chief Engineer	Deputy Chief Engineer	Center CIO
For the Office of Education	Deputy Assistant Administrator for Education	Center CIO
For Office of the CFO	Deputy CFO	Deputy CFO

Figure 14-1 Authorizing Officials

14.5.2 AOs for master systems shall:

a. Make the security accreditation decisions for their master systems, which establish the IT security posture of the associated subordinate systems. See NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, Appendix E, for sample accreditation decision letters.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. Advocate to the NASA CFO and CIO that funding be redirected to implement security controls required for master or subordinate systems to achieve full ATO.

d. Concur or non-concur on the determination of the master system's boundaries, the IT security category, the information type, the initial risk assessment, and the selection of security controls which will be inherited by any subordinate system under the authority of the master system.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

14.5.3 AOs for subordinate systems shall:

a. Make the security accreditation decisions for the subordinate systems, which inherits the IT security posture of the associated master system.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA CFO and CIO that funding be redirected to implement security controls required for the subordinate systems to achieve full ATO.

d. Concur or non-concur on the system's boundaries, the IT security category, the information type, the initial risk assessment, and the selection of security controls inherited from the master system. Non-concurrences shall indicate that the system should be aligned with a different master or that a new master system must be created.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

14.5.4 A full ATO shall be granted for only three years after which the system shall undergo another certification and accreditation process. The outcome could be a new ATO or an IATO, extension to the existing ATO, or the requirement to halt operations. Requests for up to a six-month extension of an existing full ATO can be submitted through the Center CIO to the NASA OCIO.

14.5.5 An IATO shall be granted for three months, with one extension allowed for an additional three months. After a maximum of six months operating under an IATO, the system shall halt operations. Requests for extension of the IATO shall be submitted through the NASA OCIO and the Office of the Deputy Administrator.

14.5.6 The NASA SAISO and Center ITSMs shall be prohibited from performing the security accreditation decision.

14.6 Additional Certification and Accreditation References

a. NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems.

b. NIST SP 800-30, Risk Management Guide for Information Technology System.

c. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

SECTION IV OPERATIONAL CONTROLS

a. Once the requirements for a system have been defined, other factors must be considered to ensure the security of that system. Operational controls are controls that are implemented and executed by people, as opposed to systems. These controls are implemented to improve the security of a particular system or group of systems. They often require technical or specialized expertise and often rely upon management activities, as well as technical controls.

b. Requirements for operational controls include personnel and user issues, contingency planning, configuration management, computer support and operations, incident handling, and IT security awareness and training. Additional information on personnel screening and physical and environmental controls can be found in NPR 1600.1, NASA Security Program Procedural Requirements.

Chapter 15 System Contingency Planning

15.1 Contingency Planning

15.1.1 NASA shall follow the contingency planning guidance in NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

15.1.2 It is critical that the services provided by NASA's information and technology resources and their associated information infrastructure are able to operate effectively without excessive interruption.

15.1.3 IT contingency planning refers to the coordinated strategy that involves plans, procedures, and technical measures that enable the recovery of an IT system or systems and the associated operations and data after a disruption in service.

15.1.4 The contingency planning strategy encompasses several different types of contingency plans, each with its own focus. NASA's goal is to use the contingency planning process to prepare response, recovery, and continuity activities to avert disruptions affecting NASA's most critical business processes. Because there is an inherent relationship between an IT system and the business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

15.1.5 Contingency planning should be documented at a level appropriate to a coordinated response. To avoid duplication of effort and uncoordinated response, lower-level elements of the response should reference the plan and document only internal contingency measures that are not needed to be visible to interdependent systems.

15.1.6 Although there are many types of contingency plans, each master or subordinate system need only address the subset necessary for that system. Contingency plans shall be incorporated into the

SSP.

15.2 Business Impact Analysis

15.2.1 NASA shall:

a. Follow NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, Appendix B, for Business Impact Analysis (BIA).

b. Follow NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, Appendix A, to create each system's contingency plan.

15.2.2 The BIA is considered a key step in the contingency planning process. The BIA enables the information system owner and the information owner to fully characterize the system requirements, processes, and interdependencies and to use this information to determine contingency requirements and priorities for NASA's most critical business processes and the supporting IT services.

15.2.3 The BIA correlates specific system components with the critical services that they provide, and based on that information, characterizes the consequences of a disruption to the system components. Results from the BIA will be appropriately incorporated into the analysis and strategy development efforts for the organization's Contingency Plan, Continuity of Operations Plan, Business Continuation Plan, and Business Resumption Plan.

15.3 Contingency Planning Requirements

15.3.1 NASA contingency planning processes shall:

a. Encompass response, recovery, and continuity activities to avert disruptions affecting NASA's most critical business processes.

b. Ensure that all NASA IT systems have a coordinated contingency strategy that involves plans, procedures, and technical measures that enable the recovery of an IT system or systems and the associated operations and data after a disruption in service.

c. Develop, implement, and annually test contingency plans and procedures that:

(1) Ensure continuity of operations for information systems that support the operations and assets of the Agency consistent with the information systems' risk assessments. This includes notification and activation procedures, recovery operations, and "return to normal" processes.

(2) Meet the needs of the organization and its requirements, including customer expectations.

(3) Provide established procedures to recover a system following a disruption in service.

(4) Can stand alone.

(5) Contain detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption and would serve as a "user's manual" for executing the recovery strategy to restore normal processing.

(6) Document technical capabilities designed to support contingency operations.

(7) Balance detail with flexibility; usually the more detailed the contingency plan is, the less scalable and versatile the approach.

(8) Call for the review of accounts at least annually.

(9) Appear as a section of the security plan or as a separate document with a copy attached to the plan as an appendix, depending on the size and complexity of the system.

(10) Provide quick and clear direction in the event personnel unfamiliar with the plan or the systems are called on to perform recovery operations that are clear, concise, and easy to implement in an emergency.

(11) Use checklists and step-by-step procedures where possible. A concise and well-formatted plan reduces the likelihood of creating an overly complex or confusing plan.

(12) Address any assumptions made in the contingency plan, such as the assumption that all key NASA personnel would be available in an emergency. However, assumptions should not be used as a substitute for thorough planning. For example, the contingency plan should not assume that disruptions would occur only during business hours; by developing a contingency plan based on such an assumption, the Contingency Planning Coordinator (CPC) might be unable to recover the system effectively if a disruption were to occur during non-business hours. The CPC:

(i) Is typically a functional or resource manager.

(ii) Develops the strategy in cooperation with other functional and resource managers associated with the system or the business processes supported by the system.

(iii) Manages development and execution of the contingency plan.

(iv) Identifies and coordinates with internal and external points of contact (POC) associated with the system to characterize the ways that they depend on or support the IT system, including organizations that provide or receive data from the system, as well as contacts supporting any interconnected systems.

(v) Evaluates the system to link these critical services to system resources.

d Ensure that the guidance provided by NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedures and Guidelines, is followed for IT systems that are identified as MEI.

15.4 Additional System Contingency Planning References

a. NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedures and Guidelines.

b. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

Chapter 16 Network and Systems Monitoring

16.1 Monitoring of Electronic Data on NASA Computer Networks

16.1.1 Monitoring of computer network traffic refers to the capture of electronic data while in transit or in storage and the subsequent inspection of protocols, ports, and contents of data packets, either in its raw or reconstituted form.

16.1.2 Purpose of Monitoring

16.1.2.1 NASA will continuously monitor electronic communications to ensure the productivity of its workforce, to gauge the performance and availability of its networks and services, and to secure its data and information systems from hostile intrusions, misuse, and other threats.

16.1.2.2 The monitoring (encrypted or unencrypted) of inbound or outbound traffic on any NASA network will be based on risk management principles, with a higher concentration on those assets deemed most critical to NASA.

16.1.2.3 NASA's IT resources are the property of the U.S. Government. Therefore NASA maintains the right to monitor all aspects of computer usage at any time. NASA policy states clearly that employees, including civil servants, support service contractors, grantees, and students do not have any expectation of privacy in any message, file, image or data created, sent, retrieved, or received by use of Government resources.

16.1.3 Routine Monitoring Requirements

16.1.3.1 IT security staff shall conduct continuous monitoring of NASA networks at multiple locations to ensure availability of networks and services and to detect and protect the network against hostile intrusions, misuse, and other threats.

16.1.3.2 Monitoring can include ports, IP addresses, protocols, and content. Monitoring shall be performed either by automated means, such as intrusion detection systems and flow-based content monitors, or by manual inspection of the contents of captured network data or log data. A diverse and dynamic range of computer tools are used and tested to perform monitoring activities.

16.1.3.3 Types of monitoring for hostile computer activities include the following:

a. Traffic and trend analysis.

b. Monitoring for illegal software and malicious code.

c. Enforcement of IT and IT security policies.

d. Monitoring for unauthorized network devices, services, ports, or protocols.

16.1.3.4 Routine monitoring of NASA electronic communications may be performed by:

a. Center ITSMs.

b. Center IT security personnel designated by the Center CIO.

c. NASA IT security personnel designated by the SAISO.

d. IT administrators (e.g., computer systems administrators and network administrators) within the narrow scope of normal IT administrative duties on networks under their purview.

16.1.3.5 Routine monitoring to ensure workforce productivity, the availability of networks and services, and the security of data and information systems is authorized under the Electronic Communications Privacy Act.

16.1.3.6 If suspicious traffic, criminal or non-criminal, is discovered during the course of routine monitoring, incident response and/or misuse policies shall be followed. Subsequently, if targeted monitoring is required, a request shall be submitted through the appropriate management chain.

16.1.4 Targeted Monitoring Requirements

16.1.4.1 Specific and prolonged monitoring of NASA electronic communications by NASA IT or IT security personnel can be triggered by a discovery of anomalous traffic or behavior during routine monitoring, by a formal request from a manager, or by a formal request from a law enforcement organization.

16.1.4.2 Targeted monitoring may be initiated for the following reasons:

a. A higher than expected volume of network traffic is detected on an individual's system.

b. Hostile, threatening, suspicious, unauthorized, or unusual network traffic is detected.

c. Connections to known hostile or suspicious sites are identified.

d. Unauthorized services or software are detected.

e. A violation of NASA policy is detected.

f. By approved written request from a Center, the OIG, OSPP, the General Counsel, or OHCM.

g. By court order.

16.1.4.3 Targeted monitoring when warranted and approved through the appropriate procedures may be performed by:

a. Center ITSMs.

b. Center IT security personnel and IT system administrators designated by the Center CIO.

c. NASA IT security personnel designated by the SAISO.

d. NASA law enforcement organizations as part of their investigation activities.

16.1.4.4 Targeted monitoring by NASA IT and IT security personnel in support of the NASA IT security program (i.e., resulting from anomalies found during routine monitoring or operation of NASA networks and services) is authorized under the service provider exception of the Electronic Communications Privacy Act.

16.1.4.5 Targeted monitoring by NASA IT and IT security personnel at the request of the NASA OIG, OSPP, or OHCM is performed on behalf of and under the authority of the requestor.

16.1.5 Approval for Targeted Monitoring by NASA IT and IT Security Personnel

16.1.5.1 Targeted monitoring is initiated after the Center ITSM or the NASA ITSO approves a request originating from a Center, the OHCM, the OIG, or the OSPP.

16.1.5.2 All requests for targeted monitoring will be formally submitted in writing.

16.1.5.3 All requests for targeted monitoring will be transmitted and stored according to NASA policies and guidelines, based on the sensitivity of the information contained therein.

16.1.6 Targeted Monitoring for Non-Criminal Matters

16.1.6.1 Requests shall include:

a. The requestor's name, title, and contact information.

b. Specification of the monitoring target (e.g., specific computer system).

c. Specific requirements for monitoring (e.g., monitor all incoming and outgoing activity).

d. Specific requirements for storage and handling of monitoring results.

16.1.6.2 A time limit, not to exceed three months, shall be set for monitoring requests.

16.1.6.3 After three months, a review and resubmission of the request are required to extend monitoring for another three months.

16.1.6.4 At the conclusion of the monitoring activity, the ITSM and/or monitoring personnel will require a receipt acknowledging that official monitoring results were provided to the requestor.

16.1.7 Targeted Monitoring for Criminal or Counter-Intelligence Matters

16.1.7.1 Requests shall include:

a. The requestor's name, title, and contact information.

b. Official case number of the investigation being supported.

c. Specification of the monitoring target (e.g., specific computer system).

d. Specific requirements for monitoring (e.g., monitor all incoming and outgoing activity or monitor interactions from other entities across the network).

e. Specific requirements for storage and handling of monitoring results.

f. Authority under which monitoring is to be performed.

16.1.7.2 A time limit, not to exceed three months, shall be set for monitoring requests.

16.1.7.3 After three months, a review and resubmission of the request are required to extend monitoring for another three months.

16.1.7.4 At the conclusion of the monitoring activity, the ITSM and/or monitoring personnel will require a receipt acknowledging that official monitoring results were provided to the requestor.

16.1.8 Handling and Turning Over Evidence to Authorities

16.1.8.1 When performing requests for targeted monitoring on behalf of law enforcement officials such as the OIG or OSPP, monitoring personnel will be briefed by the requestor on their responsibilities and on the proper handling of monitoring results. Monitoring personnel may be asked to sign a non-disclosure agreement.

16.1.8.2 Whenever information containing results of routine or targeted monitoring activity is furnished, the ITSM and/or monitoring personnel will obtain a receipt from the official requestor. A record will be kept of all authorities and requesters receiving evidence.

16.1.9 Records Requirements

16.1.9.1 Information collected from routine and targeted monitoring shall be properly safeguarded and not released beyond the Center CIO, ITSM, and the monitoring personnel unless approved by the Center CIO and/or SAISO.

16.1.9.2 All releases of this data to a third party must be documented. Data collected during monitoring shall be stored by monitoring personnel in accordance with NASA records management policies. Law enforcement officers and other requesters will identify in their request any additional storage and handling requirements.

16.1.9.3 Law enforcement officials shall be responsible for storing and safeguarding data collected during targeted monitoring once this data has been furnished to them.

16.1.10 Research of New Monitoring Technology

16.1.10.1 To maintain an effective and current IT security capability, NASA may occasionally develop or evaluate new monitoring tools or technology within the NASA environment. NASA will ensure that such testing, verification, and validation of monitoring technology not violate NASA policies and guidelines, nor endanger NASA resources and data.

16.1.10.2 In the course of testing, verifying, and validating monitoring technology within the NASA environment, only personnel authorized under this policy will install and run monitoring tools on NASA networks.

16.1.10.3 If external third party or contract technology is used, tested, validated, and verified using NASA resources (e.g., data, equipment, software, personnel, etc.) a testing agreement and protocol shall be in place and approved by the Center CIO or SAISO or designee.

16.1.10.4 All non-NASA or non-NASA-contractor personnel involved with the evaluation or development of monitoring technology shall sign a non-disclosure agreement.

16.1.11 Responsibilities

16.1.11.1 The NASA CIO shall maintain oversight of the NASA IT security monitoring program.

16.1.11.2 The SAISO:

a. Maintains responsibility and accountability for the NASA-wide implementation of the NASA IT security monitoring program.

b. Appoints, in writing, OCIO-sponsored NASA monitoring personnel with at least a U.S. secret clearance.

c. Informs the NASA CIO, as appropriate, about monitoring activity and findings.

d. Reviews and approves testing agreements and protocols for evaluations of monitoring technology in the NASA network environment.

16.1.11.3 The NASA ITSO:

a. Develops an appropriate use policy to be signed on a yearly basis by all monitoring personnel, which strictly forbids the sharing of all monitoring data without explicit permission from the appropriate NASA officials.

b. Reviews and approves requests for targeted monitoring from authorized NASA managers and law enforcement officials.

c. Informs NASA managers and the NASA SAISO as appropriate on the results of targeted monitoring.

16.1.11.4 The Center CIO:

a. Maintains responsibility and accountability for Center-specific implementation of the NASA IT security monitoring program.

b. Appoints, in writing, Center monitoring personnel with at least a U.S. secret clearance.

c. Informs the Center Director, as appropriate, of monitoring activity and findings.

d. Reviews and approves testing agreements and protocols for evaluations of monitoring technology in the Center network environment.

16.1.11.5 The Center ITSM:

a. Reviews suspicious activities identified during routine monitoring to determine the course of action (e.g., whether activity appears criminal and warrants notification of law enforcement; whether non-criminal but suspicious activity warrants escalation to targeted monitoring and/or notification of other entities).

b. Notifies law enforcement of suspected criminal activities identified during monitoring.

c. Reviews and approves requests for targeted monitoring from authorized NASA managers and law enforcement officials.

d. Maintains documentation of all targeted monitoring activities involving the Center, including law enforcement or other requests for targeted monitoring and receipts for targeted monitoring records.

e. Ensures that all data collected from monitoring is properly safeguarded.

f. Informs NASA managers and the Center CIO as appropriate on the results of targeted monitoring.

g. Ensures that all monitoring personnel sign an appropriate use policy on a yearly basis, which strictly forbids the sharing of all monitoring data without explicit permission from appropriate NASA officials.

16.1.11.6 NASA and Center monitoring personnel:

a. Conduct monitoring as directed under the NASA IT security monitoring program.

b. Maintain audit logs of all routine monitoring activities, as well as identified suspicious activities recommended for further targeted monitoring.

c. Report to the Center ITSM or other appropriate management chain any suspicious activity identified during routine monitoring.

d. Provide technical support and monitoring services for approved targeted monitoring activities.

e. Inform the Center ITSM or NASA ITSO as appropriate on the progress and results of targeted monitoring.

f. Provide records of approved targeted monitoring to the requestor.

g. Properly safeguard all data collected from monitoring.

16.1.11.7 The NASA Deputy Inspector General shall review and validate all requests for targeted monitoring from the OIG to ensure they meet legal and administrative requirements.

16.1.11.8 The NASA Deputy Associate Administrator for Security and Program Protection shall review and validate all requests for targeted monitoring from the OSPP to ensure they meet legal and administrative requirements.

.

16.2 Periodic Testing and Security Controls Assessment

16.2.1 It is not feasible or cost-effective to monitor all of the security controls in an information system on a continuous basis. Therefore, each information system owner is required to use an appropriate subset of controls for periodic assessment and identify the frequency of such monitoring activity. The selection and frequency of testing are determined by the sensitivity and importance of the information system to NASA operations, NASA assets, or individuals.

16.2.2 Periodic Testing and Assessment of Security Controls Requirements

16.2.2.1 Information system owners shall conduct annual testing and assessment of the system security controls to assure effective controls.

16.2.2.2 Information system owners shall develop and maintain a prioritized list of security controls to be monitored, based on the results of the risk determination.

16.2.2.3 Information system owners shall maintain a list of security controls for periodic testing which contains the following information:

a. Priority, stated as one of the following levels as determined by the risk determination:

(1) High impact and high likelihood.

(2) High impact and moderate likelihood.

(3) Moderate impact and high likelihood.

(4) Moderate impact and moderate likelihood.

(5) High impact and low likelihood.

b. Security Control name.

c. Brief description of the control as it relates to the information system security level.

d. Brief description of the control objective.

e. Frequency of periodic assessment (i.e., quarterly, semiannual, annually).

16.2.2.4 The list of security controls to be monitored will be approved by:

a. System's AO and the NASA SAISO for the set of security controls for each master system plan.

b. System's AO and the Center CIO for the set of security controls for each subordinate system plan.

16.3 Continuous Monitoring Requirements

16.3.1 In addition to the continuous monitoring requirements in NIST SP 800-37, NASA systems shall:

a. Ensure that a self-assessment of each system is performed at least annually using the NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, and ITS-SOP-0005-B, Procedure for Completing a NASA IT Security Program or System Assessment.

b. Ensure that an intrusion detection system (IDS) capability is implemented and maintained to monitor traffic continually at the Network Security Perimeter (NSP) for security, performance, traffic analysis, and vulnerabilities.

c. Ensure that a full Center site survey is performed at least semiannually to detect unauthorized WLAN access points and to ensure that spot checks are performed quarterly.

16.4 Network Testing and Vulnerability Scanning

16.4.1 Despite the best efforts to include security measures and implement security controls in a system or application, there is no guarantee that these measures and controls will reliably prevent security incidents over time. Network testing and vulnerability scanning is one way to determine how well security measures and controls work at a particular point in time. The results of vulnerability scanning are very sensitive and, if not conducted under strict procedures, may affect the network or systems. Vulnerability scanning only determines the vulnerabilities that exist on a computer system without actually circumventing security processes and controls of the system being scanned.

16.4.2 NASA shall follow NIST SP 800-42, Guideline on Network Security Testing.

16.4.3 Network security testing and vulnerability scanning shall only be conducted with approval of the cognizant Center ITSM .

16.4.4 The NASA CIO shall issue directives for the scanning, elimination and mitigation, and reporting on specific high-risk vulnerabilities. The specific high-risk vulnerabilities shall be identified for scanning by the CCITS Manager in coordination with the Center ITSMs. The SAISO, CCITS Manager, and Center ITSM shall develop and maintain NASA ITS-SOP-0021, Vulnerability Scanning Procedures, on how vulnerabilities scanning is to be accomplished.

16.4.5 Results from network vulnerability scanning shall be marked and handled as ACI or SBU information.

16.5 Configuration Management

16.5.1 System security planned security controls need to be managed and maintained through configuration control processes. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, provides additional information on the importance of configuration management. All NASA systems shall use the Agency's operating system and application configuration benchmarks.

16.5.1.1 IT security configuration management provides assurance that the system is the intended version (configuration) and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security. Changes to an information resource may present security implications because they may introduce or remove vulnerabilities and because significant changes may require updating the IT security plan or contingency plan, performing a risk analysis, and recertifying and accrediting the system.

16.5.1.2 The main security goal is to determine and document what changes occur, not to prevent security from being changed. A second security goal of configuration management is to ensure that changes to the system are reflected in other documentation, such as the contingency plan. If the change is major, it will be necessary to reanalyze and document some or all of the system's security controls.

16.5.2 Hardware and Software Configuration Management Process Requirements

16.5.2.1 Hardware and software configuration management activities shall ensure that:

a. A configuration management policy and process that defines software and hardware standards for IT systems is developed and implemented.

b. A configuration management process is in place for each of their IT systems, including an approval and signoff process for changes to their IT systems (e.g., system enhancement, major changes to the software and hardware).

c. Standards are defined and maintained for IT systems.

d. Changes to a system do not diminish its security or functionality.

e. Current best practices for configuration management of major operating system types are published.

f. An effective patch management program is implemented and maintained that includes verification that patches have been properly applied to all systems.

g. An effective vulnerability reduction program to include periodic scanning for critical high-risk vulnerabilities is implemented and maintained.

16.5.3 Standard Operating System Process Requirements

16.5.3.1 The SAISO shall provide a mechanism to ensure that all IT resources comply with standard operating system benchmark templates. NASA will evaluate each system's operating system through a vendor-provided benchmarking capability.

a. All newly released benchmarks will be evaluated each year in October and May by the OCIO. Centers have four weeks to review benchmarks that are proposed for adoption.

b. To demonstrate compliance during reviews, Centers should ensure that their IT security plans document all deviations from the benchmarks. A complete list of available benchmarks will be made available by the vendor.

16.5.4 Network Configuration Control Board Requirements

16.5.4.1 The NCCB shall:

a. Ensure a level of risk relative to security and integrity of Center networked resources, which meets or exceeds Agency and Center requirements and expectations while maintaining an IT environment.

b. Be chaired by the Center CIO or designee.

c. Ensure that network security is addressed and will establish IP address management requirements.

d. Implement a secure process to adjudicate requests for access through the NSP for presentation to the NCCB.

e. Assign and manage all IP addresses including non-routable IP addresses behind firewalls or NAT boxes.

f. Maintain an up-to-date record of all NASA Integrated Services Network (NISN)-NISN-assigned IP addresses.

g. Monitor and document the Center's and Project's IP address ranges to ensure that Agency and Center policies have been addressed and any risk acceptance has been documented and authorized, as appropriate.

h. Ensure that security or vulnerability information on specific IP addresses is protected as ACI or SBU.

i. Have the authority to adjust bandwidth limits for traffic, including traffic between wireless access points and wired networks.

j. Report progress through the Center ITSM and SAISO.

k. Ensure the Center network is in compliance with Agency-networking standards.

l. Be subordinate to the Agency NSCB.

16.5.4.2 The Agency Network Security Control Board (NSCB)

16.5.4.2.1 The Agency NSCB shall:

a. Assure risk is mitigated to a level that maintains the security and integrity of Agency-networked resources, meets or exceeds Agency and Center requirements and expectations, and maintains a viable and secure IT environment.

b. Be chaired by the Deputy CIO for IT Security or his designee.

c. Have representation by each Center NCCB.

d. Ensure that network security is addressed at an Agency-level.

e. Implement a secure process to adjudicate requests for access through multiple Centers' NSPs or through the Agency NSP.

f. Report progress to the OCIO and CIO Board.

g. Recommend and review SOP technical standards and policies for implementation and operation of IT resources on NASA's networks.

h. Approve any change to the Agency Network Security Perimeter.

16.6 Additional Network and System Monitoring References

a. NPR 1441.1, NASA Records Retention Schedules.

b. NPD 1660.1, NASA Counterintelligence (CI) Policy.

Chapter 17 Security Incident Handling and Reporting

17.1 Incident Handling and Reporting

17.1.1 NASA shall use NIST SP 800-61, Computer Security Incident Handling Guide, for additional guidance on security incident handling.

17.1.2 IT security incident response is a critical component of the NASA Information Technology Program. Incidents require close coordination among all affected NASA operations and programs to ensure that the response is appropriate.

a. The Center ITSM and incident response staff shall make a good faith effort to coordinate with system owners in determining when IT security incidents are placing NASA's missions, its customers, its reputation, or its assets in jeopardy to a degree that the Center must exercise its responsibility to unilaterally control or terminate an incident.

b. NASIRC shall continue to be the central coordination and analysis facility for incidents germane to IT security. As an authoritative repository for incident information, the NASIRC database will be used for Center and/or Agency management reports produced for internal use or external reporting.

17.1.3 An IT security incident is an adverse event or situation associated with a system that poses a threat to the integrity, availability, or confidentiality of the information or the system and results in:

a. A failure of security controls.

b. An attempted or actual compromise of information.

c. The waste, fraud, abuse, loss, or damage of Government property or information.

17.1.4 In some cases, these events may involve violations of Federal or State laws. Due to the evolving nature of laws, policies, and requirements regarding handling and reporting of information and information system incidents, detailed procedures shall be maintained by the OCIO in concert with the OIG.

17.2 Incident Handling and Reporting Requirements

17.2.1 The ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting, shall be coordinated with the OSPP and the OIG. The SOP shall conform to Federal and NIST guidance and requirements.

17.2.2 To track trends and meet Federal reporting requirements, incidents shall be categorized by the guidelines published in NIST SP 800-61, Computer Security Incident Handling Guide. The Incident Classification Framework in Figure 17-1 defines the current incident categories.

Incident Category	Definition	Clarification
Denial of Service	An explicit attack on NASA systems that prevents or impairs the authorized use of networks, systems, or applications.	Includes only those attacks that deny service to NASA systems (i.e., inbound attack on NASA systems or packet flood affecting NASA systems that was a result of malicious code).
Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity (e.g., mobile code) that infects hosts at NASA.	Includes infections that result in an outbound Denial of Service attack that originates on NASA networks and attacks an external party.

Unauthorized Access	A person gains logical or physical access without permission to a NASA network, system, application, information, or other resource.	The emphasis is on human intervention that enables access and, therefore, this category does not include malicious code that gains system or user privileges. These attacks will be further categorized as: System Compromise and User Compromise
Misuse	A person violates acceptable computing use policies.	
Multiple Component	An incident that falls into several incident categories at once and several exploit vulnerabilities are utilized (not just available).	A virus that creates a backdoor should be handled as a malicious code incident, not an unauthorized access incident, because the malicious code was the only transmission mechanism used. A virus that creates a backdoor that has been used to gain unauthorized access should be treated as a multiple component incident because two transmission mechanisms were used.

Figure 17-1 Incident Classification Framework

17.2.3 All NASA network, Center, program, project, and system-level procedures for detecting, reporting, and responding to IT security incidents or suspected incidents, as described in Figure 17-1, shall comply with

ITS-SOP-0015, Procedures for Agency IT Security Incident Classification and Reporting.

17.2.4 All NASA contracts, cooperative agreements, grants, partnership agreements, agreements with international partners, university partners, and other educational entities, NASA Space Act Agreements, and special volunteer partners, whether funded or not funded, shall report IT security incidents and suspected incidents to the NASA sponsor and the Center ITSM. All communication about incidents transmitted between ITSMs, the CCITS Manager, Center Chiefs of Security, NASIRC, and NSOC personnel shall be encrypted.

17.2.5 Once an incident has been confirmed, Centers shall, within two hours, provide the following information to NASIRC in an encrypted and secure manner:

a. Type of incident to include system compromise, user compromise, unauthorized access, malicious code, and denial of service.

b. An initial report containing as much information as possible including:

(1) Exploited IP addresses;

(2) Hostile IP address and domain name;

(3) Exploit used;

(4) Date and time of discovery;

(5) Date and time of exploit;

(6) Operating system with version number;

(7) Incident summary;

(8) Information types of the computers affected;

(9) Labor hours and cost of downtime; and

(10) Identification of the SSP for the exploited system.

17.2.6 The Center ITSM shall determine the incident or suspected incident's severity and potential impact on NASA's overall IT security.

a. If the Center ITSM is concerned that an incident's severity and/or potential impact on NASA's overall IT security is great, they should immediately confirm with NASIRC.

b. NASIRC should immediately notify the CCITS Manager and/or the NASA Security Operations Center (NSOC) of the incident and provide suggested remedial measures to be taken.

c. If NASIRC is not available, then the process automatically defaults to the NSOC who should continue the elevation process.

d. If the severity is suspected but not confirmed, the Center ITSM or designee must immediately seek guidance from the CCITS Manager, who will determine whether the IT security emergency process should be activated and/or strong measures are to be taken.

e. The Center ITSM shall notify the CCS and CI agent and the local OIG as soon as possible, but no later than twenty-four hours after the initial analysis.

17.2.7 Centers should populate all additional relevant fields in the NASIRC database and ensure that incidents are closed within 30 days of being reported.

a. Incidents will remain open until all information requested above is provided. Once all information has been provided, the incident will be closed.

b. Centers must provide a written justification for any incident required to remain open for more than 30 days.

c. If the justification for the extension is valid, NASIRC will present the justification to the NASA SAISO for a 30-day extension.

d. NASIRC will provide weekly updates of information not available during the preparation of the initial report.

17.2.8 Information about incidents or suspected incidents shall be handled as ACI or SBU information. IT security staff working on incidents or suspected incidents shall not disclose any information regarding inquires into incidents or suspected incidents without consent from the Center ITSM or CIO.

17.2.9 Release of incident information to those outside the NASA ITSMs, CCS, OSPP, or OIG shall be handled only by the NASA Headquarters Public Affairs Office.

17.2.10 NASIRC shall:

a. Aggregate, analyze, and provide to the Agency CIO management reports on the Center's incidents.

b. Provide insight into the nature, frequency, cost, and vector of incidents.

c. Report all IT security incidents to FedCIRC within one hour of receiving a report from a Center.

17.2.11 NASA Security Operations Center (NSOC) shall:

a. Prepare a report to improve the Center's situational awareness of hostile probe activity.

b. Provide aggregated reports to the OCIO, as directed.

17.2.12 NSOC and NASIRC shall:

a. Meet once monthly via telecom to discuss any discernable patterns and/or trends in hostile probe activity and reported incidents.

b. Discuss findings with the SAISO and, if appropriate, with the weekly ITSM teleconferences.

17.2.13 The IT Security Emergency process will be tested for after-hours notification on a quarterly basis. The test will be unannounced and will be initiated by the Manager of the CCITS.

a. NASIRC will commence the call-down within 10 minutes of the test's initiation.

b. All Centers will respond within thirty minutes of receiving NASIRC's notification.

c. The manager of the CCITS will assess NASIRC's and the Centers' responsiveness and report a pass or fail status along with their cumulative time.

17.3 Additional Security Incident Handling and Reporting References

a. NIST SP 800-61, Computer Security Incident Handling Guide.

b. NASIRC Procedures for Agency IT Security Incident Classification and Reporting.

Chapter 18 IT Security Awareness and Training

18.1 Awareness and Training

18.1.1 NASA shall follow the guidance in NIST SP 800-16, IT Security Training Requirements: A Role- and Performance-Based Model, and NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, to provide IT security training for its employees. This approach prescribes the IT security training needed to provide employees with the IT security knowledge required for them to manage, acquire, design and develop, implement and operate, review, evaluate, and use NASA's information resources.

18.1.2 A knowledgeable and skilled workforce is required to ensure IT security policies and requirements are understood and implemented. NASA management will ensure that a robust and Mission Directorate-wide annual NASA IT security awareness and training program be provided. The IT Security Awareness and Training Program will ensure that all personnel, including support service contractors and other users of information systems that support the operations and assets of the Agency, be involved in using, managing, and administering information resources:

a. Understand their roles and responsibilities regarding IT security.

b. Understand NASA's IT security policies, procedures, and practices; and have adequate knowledge of the various management, operational, and technical controls required and available to protect IT resources for which they are responsible.

18.2 Awareness and Training Requirements

18.2.1 NASA civil service employees, support service contractors, and grantees, and those who use, manage, or administer NASA information resources will pass all required IT security awareness training modules annually. Additional IT security awareness and training, as defined annually by the SAISO, is required of key management, system administrators, and network administrators, who are civil service employees, contractors, or grantees.

18.2.2 All NASA contracts, cooperative agreements, grants, partnership agreements, agreements with international partners, university partners, and other educational entities, NASA Space Act Agreements, purchase orders, purchase-card buys, inter-governmental orders, and special volunteer partners, whether funded or not funded, shall establish and budget for an aware and skilled workforce in IT security relating to individual roles and responsibilities.

18.2.3 Centers shall coordinate with the IT Security Awareness and Training Center and should ensure the certification of all system administrators.

18.2.4 The IT Security Awareness and Training Center will aggregate and summarize the Agency's overall training status.

18.3 Additional Awareness and Training References

a. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.

SECTION V TECHNICAL CONTROLS

a. The technical controls focus on security controls that the IT system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization.

b. Technical controls are installed, maintained, and used by support and operations staff. This staff has the responsibility to create the user accounts, add users to access control lists, review audit logs for unusual activity, control bulk encryption over telecommunications links, and perform the countless operational tasks needed to use technical controls effectively. In addition, the support and operations staff provides needed input to the selection of controls based on their knowledge of system capabilities and operational constraints.

Chapter 19 Account Management

19.1 Identification and Authentication

19.1.1 Identification and authentication (I&A) is a critical building block of IT security. I&A is the basis for access control and a mechanism for establishing user accountability for NASA. I&A is a technical control to prevent unauthorized people or processes from gaining access to NASA information or information systems. The system must be able to identify and differentiate among the diverse set of NASA users if access control is to work effectively. In addition, the approaches implemented must be compliant with Federal laws, regulations, and requirements.

19.1.2 Identification is a means by which a user provides a claimed identity to the system. Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors, requires the use of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors.

19.1.3 NASA information and information system owners are required to ensure that their applications, including COTS applications, are implemented utilizing FIPS 201 for identification, as well as to migrate their existing applications to use FIPS 201 following NASA's HSPD-12 Implementation Plan.

19.2 Account Management Requirements

19.2.1 NASA application and service providers are required to integrate their applications with the NASA account management and identity management systems. The NASA Account Management and Identity Management Systems will provide the NASA common infrastructure necessary to support the Federal E-Authentication and HSPD-12 requirements.

19.2.2 The NASA Account Management System (NAMS) will provide a central management system and repository of account information. This includes:

a. A single Agency infrastructure to provide account management services and support.

b. A reliable source of user access information for account provisioning.

c. Elimination of duplicative user account information and administration.

d. Enforcement of uniform security and auditing standards for account access.

e. Termination of physical and logical access to IT resources promptly and reliably.

f. A consistent process for establishing and managing accounts across all NASA Centers and installations.

g. Definition of account management metrics in the system operations documentation.

Chapter 20 Logical Access

20.1 Logical Access Overview

20.1.1 Logical access controls are the system-based means by which the ability to do something with an information resource is explicitly-enabled or restricted in some way. Logical access controls prescribe not only who or what, in the case of a process, is to have access to a specific system resource, but also the type of access that is permitted. Five methods of logical access control are passwords, encryption, access control lists, constrained user interfaces, and labels.

20.1.2 Logical access controls may be built into the operating system, may be incorporated into programs or major utilities (e.g., database management systems or communications systems), or may be implemented through add-on security packages. Logical access controls may be implemented internally to the IT system being protected or may be implemented in external devices.

20.1.3 External access controls are a means of controlling interactions between the system and outside people, systems, and services. External access controls use a wide variety of methods, often including a separate physical device (e.g., a computer) that is between the system being protected and a network.

20.2 Logical Access Requirements

20.2.1 NASA shall ensure that all access controls identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented including, but not limited to:

a. Implementing logical access controls on NASA systems and applications based on impact levels, policy, and permissions established by the management official responsible for the particular system, application, subordinate systems, or group of systems.

b. Basing access control policy on the principle of least privilege.

c. Weighing the potential impacts, costs, and benefits to the Government as a risk decision before granting any IT access.

d. Implementing an auditable process exists for granting, establishing, and maintaining users' accounts.

e. Ensuring that the user's identity is unique in order to support individual accountability.

f. Considering the job assignment of the user who is seeking access to NASA IT resources in the control of access to information.

20.3 Additional Logical Access References

a. NIST SP 800-12, Introduction to Computer Security: The NIST Handbook.

b. NIST SP 800-19, Mobile Agent Security.

c. NIST SP 800-28, Guidelines on Active Content and Mobile Code.

Chapter 21 Audit Trails and Accountability

21.1 Audit Trails and Accountability Overview

21.1.1 An audit trail is a series of records of IT events about a user, an application, or an operating system. Audit trails are designed to capture and maintain a record of system activity.

21.1.2 The NASA ITS Program requires that audit trails, used in conjunction with the appropriate tools and procedures, shall be collected and utilized for individual accountability, reconstruction of events, intrusion detection, and problem identification.

21.2 Audit Trail and Accountability Requirements

21.2.1 NASA shall ensure that all audit trail and accountability requirements identified in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, have been implemented.

21.2.2 NASA shall ensure that:

a. Audit trails are implemented on all NASA IT systems. The amount of detail logged shall be commensurate with the system's information category and impact level.

b. The confidentiality of the audit trail information is protected as ACI or SBU, according to the guidelines in NPR 1600.1, NASA Security Program Procedural Requirements.

c. Audit trails are reviewed periodically, with the frequency of these reviews and retention schedules being consistent with the security category of the system.

d. Access to on-line audit logs is strictly controlled.

e. There is a separation of duties between security personnel who administer the access control function and those who administer the audit trail. This is a requirement for high and moderate impact systems and strongly recommended for low impact systems.

21.3 Additional Audit Trail and Accountability References

a. NIST SP 800-12, Introduction to Computer Security: The NIST Handbook.

b. NIST SP 800-31, Intrusion Detection Systems.

SECTION VI APPENDICES

Appendix A Acronym List

AAO	Account Authorization Official
ACI	Administratively Controlled Information
AO	Authorizing Official
ATO	Authorization to Operate
BIA	Business Impact Analysis
CA	Certification Agent
C&A	Certification and Accreditation
CCITS	Competency Center for IT Security
CCS	Center Chief of Security
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CI	Counterintelligence
CIO	Chief Information Officer

CNSI	Classified National Security Information
COOP	Continuity of Operations
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf
CPC	Contingency Plan Coordinator
CPIC	Capital Planning and Investment Control
CSPA	Cost, Schedule, and Performance Agreement
DAA	Designated Approval Authority
DVD	Digital Video Disk
EO	Executive Order
E-Mail	Electronic Mail
FAD	Formulation Authorization Document
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GOCO	Government Owned, Contractor Operated
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act

HSPD	Homeland Security Presidential Directive
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authorization
IA	Independent Assessments
IAO	Information Assurance Officer
IAR	Independent Assessment Review
IATO	Interim Authorization to Operate
IDS	Intrusion Detection System
IEEE	Institute for Electrical and Electronics Engineers
IP	Internet Protocol
ISPO	Infrastructure Service Provider Organization
IRM	Information Resource Management
ISP	Internet Service Provider
ISSO	Information System Security Official
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITMRA	Information Technology Management Reform Act
ITS	Information Technology Security
ITSM	Information Technology Security Manager

LAN	Local Area Network
MA	Major Application
MAC	Media Access Control
MEI	Mission Essential Infrastructure
MOU/MOA	Memorandum of Understanding/Agreement
NAMS	NASA Account Management System
NAR	Non-Advocate Review
NASIRC	NASA Incident Response Center
NAT	Network Address Translation
NCCB	Network Configuration Control Board
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NODIS	NASA Online Directives Information System
NPD	NASA Policy Directive
NPR	NASA Procedures and Requirements
NRA	NASA Research Announcement
NSA	National Security Agency
NSCB	Network Security Control Board

NSM	NASA Structure Management
NSOC	NASA Security Operations Center
NSP	Network Security Perimeter
NTISS	National Telecommunications and Information System Security
OAIT	Office Automation of Information Technology
OCIO	Office of the Chief Information Officer
OCSO	Organization Computer Security Official
OHCM	Office of Human Capital Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSPP	Office of Security and Program Protection
PAA	Principle Accreditation Authority
PCA	Program Commitment Agreement
PDD	Presidential Decision Directive
PMA	President's Management Agenda
POA&M	Plan of Actions and Milestones
P2P	Peer-to-Peer
PUB	Publication
RFI	Request for Information

RFP	Request for Proposal
RFQ	Request for Quotation
ROM	Read Only Memory
SAISO	Senior Agency Information Security Officer
SBU	Sensitive But Unclassified
SDLC	System Development Life Cycle
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SOW	Statement of Work
SP	Special Publication
SSP	System Security Plan
STI	Scientific and Technical Information
TCP	Transfer Control Protocol
TCP/IP	Transport Control Protocol/Internet Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
U.S.C	United States Code
VPN	Virtual Private Network
WAN	Wide Area Network

WLAN	Wireless Local Area Network

Appendix B Glossary

Term	Definition
Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.
Acceptance	The act of an authorized representative of the Government by which the Government, for itself or as agent of another, assumes control or ownership of existing identified supplies tendered or approves specific services rendered as partial or complete performance of the contract. It is the final determination whether a facility or system meets the specified technical and performance standards.
Access	Access is the ability to do something with a computer resource. This usually refers to a technical ability (e.g., read, create, modify, or delete a file, execute a program, or use an external connection).
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Accountability

The security goal that generates the requirement for actions of NASA management to be traced uniquely to a specific NASA resource. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Account Authorization Official

The NASA Center official with authority and responsibility for all aspects of policy, business operations, and operational life cycle for NAMS. The Center AAO is the primary technical representative and provides guidance and oversight of the daily activities and personnel supporting NAMS. The Center AAO represents all Center NAMS activities and operations to Agency-level committees with oversight responsibility for NAMS implementations across NASA.

Accreditation

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed upon set of security controls.

Accreditation Package

The evidence provided to a NASA authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.

Acquisition

All stages of the process of acquiring property or services, beginning with the process for determining the need for the property or services and ending with contract completion and closeout.

Active Content

Active content refers to electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user. Active content technologies allow mobile code associated with a document to execute as the document is rendered.

Adequate Security

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical controls.

Administratively Controlled Information (ACI)

Certain official information and material which is not national security information (and therefore cannot be classified), nonetheless, should be protected against disclosure. Such information and material, which may be exempt from disclosure by statute or is determined by a designated NASA official to be especially sensitive, shall be afforded physical protection sufficient to safeguard it from unauthorized disclosure. Within NASA, such information has previously been designated "FOR OFFICIAL USE ONLY." This designation has been changed for clarity and to more accurately describe the status of information to be protected. (See NPG 1620.1, Section 4.4.7 for specifics.)

Application

The use of information resources (information and information technology) to satisfy a specific set of user requirements (reference OMB A-130). Also, a set of computer commands, instructions, and procedures used to cause a computer to process a specific set of information. Application software does not include operating systems, generic utilities, or similar software that are normally referred to as "system software."

Assessment Method

A focused activity or action employed by an assessor for evaluating a particular attribute of a security control.

Assurance

Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Auditing

Auditing is the review and analysis of management, operational, and technical controls. The auditor can obtain valuable information about activity on a computer system from the audit trail. Audit trails improve the auditability of the computer system.

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Authorization

Authorization is the permission to use a computer resource. Permission is granted, directly or indirectly, by the application or information system owner.

Authorizing Official

A NASA official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals.

Availability

As defined in FISMA, the term 'availability' means ensuring timely and reliable access to and use of information [44 USC 3542 (b)(1)(C)].

Background Investigation

The means or procedures used to determine the suitability of an individual to have privileged or limited privilege access and to hold a "Public Trust" position. Conducted by the Center Chief of Security.

Baseline Set of Security Controls

The minimum security controls recommended for an information system based on the system's security categorization established in accordance with FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems (prepublication final), December 2003.

Certification

Certification is a formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer, rather than one involved in building the system. Certification is more often cost-effective for complex or high-risk systems. Less formal security testing can be used for lower-risk systems. Certification can be performed at many stages of the system design and implementation process and can take place in a laboratory, operating environment, or both.

Certification Agent

The individual, group, or organization responsible for conducting security certification.

Chief Information Officer (CIO)

Agency official responsible for: (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, and regulations, and the priorities established by the head of the agency; (2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Chief Information Security Officer

Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

Clinger-Cohen Act of 1996

A statute that substantially revised the way that IT resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of IT investments.

Common Security Control

Security control that can be applied to one or more NASA information systems and has the following properties: (1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control may have been applied.

Compromise

Disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Computer Security

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information/data, and telecommunications).

Computer Virus

A computer virus is similar to a Trojan horse insofar as it is a program that hides within a program or data file and performs some unwanted function when activated. The main difference is that a virus can replicate by attaching a copy of itself to other programs or files and may trigger an additional "payload" when specific conditions are met.

Confidentiality

The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.

Configuration Control

Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.

Contingency Plan

Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. Contingency plans assist managers to ensure that data owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

Contracting Officer

A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

Contracting Officer's Technical Representative

An individual to whom the CO delegates certain contract administration responsibilities, usually related to technical direction and acceptance issues.

Cost-Benefit Analysis

When considering security, cost-benefit analysis is done through risk assessment, which examines the assets, threats, and vulnerabilities of the system in order to determine the most appropriate, cost-effective safeguards (that comply with applicable laws, policy, standards, and the functional needs of the system). Appropriate safeguards are normally those whose anticipated benefits outweigh their costs. Benefits and costs include monetary and non-monetary issues such as prevented losses, maintaining an organization's reputation, decreased user friendliness, or increased system administration.

Counterintelligence

The term "counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities [50 USC 401a].

Countermeasures
Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Cryptographic Module
The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module [FIPS PUB 140-2].

Deliverable
A product or service that is prepared for and delivered to the Government under the terms of a contract.

Denial of Service
The prevention of authorized access to resources or the delaying of time-critical operations.

Development/Acqui-sition
During this phase the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

Disposal of Assets
Releasing the accountability (excessing, turned in for repair, or transferring to another organization) of IT equipment and ensuring the elimination of any controlled information and software stored on this equipment.

Encryption
The translation of data into a form that is unintelligible without a deciphering mechanism.

Event
Any observable occurrence in a network or system.

Exhibit 300

The Exhibit 300 business case is a high-level summary of the investment's current justification and management plans, including a project plan, benefit-cost analysis, alternatives analysis, acquisition plan, risk management plan, human resources management plan, enterprise architecture, and IT Security plan. In the case of proposed new IT investments, this information is used by the operating unit, the department's Capital Investment Technology Review Board (CITRB), and OMB to determine if the investment should be recommended for funding. For ongoing investments, the Exhibit 300 is used to review the investment's current status and, subsequently, to assess how well the investment accomplished its goals. In addition, the Exhibit 300 is required when requesting a delegation of procurement authority from the CIO through the CITRB or the Acquisition Review Board to proceed with a large contract. It is expected that the Exhibit 300 information is supported by more detailed plans for acquisition, risk management, alternatives, benefit-cost analysis, project scheduling, security and earned value management.

Exhibit 53

Section 53 describes IT portfolio data (major projects) reporting requirements and focuses on how such investments should be linked to the President's Management Agenda (PMA), E-government. "Major IT system or project means a system that requires special management attention because of its importance to an agency mission. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) should be evaluated against ["major" IT system or project] criteria... Additionally, if the project or initiative directly supports the President's Management Agenda items, then the project meets the criteria of "high executive visibility." Projects that are E-Government in nature or use e-business technologies must be identified as major projects regardless of the costs."

External Customers or Groups

Those who are not affiliated in any way with the entity with which they are conducting business. In this document, these customers may include Federal, State, or local Governments; international partners; other NASA organizations; or organizations in the private sector.

Facility

Designated locations in which a logical group of one or more IT resources are located.

Federal Information Processing Standards (FIPS)

Issued by the NIST after approval by the Secretary of Commerce regarding management and operations of IT resources. (Also called FIPS PUBS.)

FIPS PUB

An acronym for Federal Information Processing Standards Publication. FIPS publications (PUB) are issued by NIST after approval by the Secretary of Commerce. Some FIPS PUBs are mandatory for use in federal acquisitions.

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

General Support System

General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Hostile Probes

The act of using one or more systems to scan targeted systems or networks with intent to conduct or to gather information for unauthorized activities. They are often targeted against networks (LAN's) rather than single stand-alone systems. They may return information that may provide information on system vulnerabilities.

Identification

The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Intrusion Detection System

A software application that can be implemented on host operating systems or as network devices to monitor for signs of intruder activity and attacks.

Impact

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Implementation

After initial system testing, the system is installed or fielded.

Inappropriate Usage

A person who violates acceptable computing use policies.

Incident

An adverse event or situation associated with a system which poses a threat to the integrity, availability, or confidentiality of data or systems and that results in a failure of security controls; an attempted, suspected, or actual compromise of information; or the waste, fraud, abuse, loss, or damage of Government property or information.

Individual Accountability

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information

Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, such as computerized databases, paper microfilm, tapes, disk, memory chips, RAM, ROM, microfiche, communication lines, and display terminals.

Information Assurance

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities

[CNSS 4009].

Information Owner

The individual (organizational line manager) responsible for the confidentiality, integrity, and availability of a specific set of data. This individual is responsible for making judgments and decisions on behalf of the organization with regard to the data's information category level, criticality, use, protection, and sharing. Typically, this individual is a member of the organization directly supported by the data. This individual often maintains the data and ensures its accuracy. All data have a data owner.

Information Resource Management

The planning, budgeting, organizing, directing, training, and control of information and related resources, such as personnel, equipment, funds, and technology.

Information Security Policy

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System

The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems are also referred to as IT systems within this document.

Information System Security Official

The principal staff advisor to the information system owner on all matters involving the ITS of the information system. This responsibility may also include physical security, personnel security, incident handling, and security training and education.

Information Technology

The term "information technology," with respect to an executive agency, means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Information Technology Resources

Data and information; computers, ancillary equipment, software, firmware, and similar products; facilities that house such resources; services, including support services; and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data. This includes telecommunication systems, network systems, and human resources. (Also called Automated Information Resources.)

Information Technology (IT) System

See information system.

Information Type

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity - Accountability

The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to: Accountability. A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Integrity - Authenticity

Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to: Authenticity. A third party must be able to verify that the content of a message has not been changed in transit.

Integrity - Non-repudiation

The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to: Non-repudiation. The origin or the receipt of a specific message must be verifiable by a third party.

Integrity [44 U.S.C., Sec. 3542]

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Intelligence

The term "intelligence" means (1) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term "intelligence" includes foreign intelligence and counterintelligence [Joint Pub 1-02] [50 USC Ch 15].

International Partner

Foreign entities with which business and/or research is conducted. International partners may include individuals, small firms, large corporations, and/or foreign governments.

Internet Protocol (IP)

A standard designed for use in interconnected systems of packet-switched computer communication networks. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fix-length addresses.

Intrusion Detection

Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.

Intrusion Detection System (IDS)

A software application that can be implemented on host operating systems or as network devices to monitor activity that is associated with intrusions or insider misuse, or both.

IP address

An IP address is a unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.

Information Owner

An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information System Owner

An agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. Responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the security requirements.

Information System Security Official

The information system security official (ISSO) is the principal staff advisor to the information system owner on all matters involving the IT security of the information system. This responsibility may also include physical security, personnel security, incident handling, and security training and education. For smaller systems, a system administrator may perform the ISSO role as well as the system administrator role.

Keystroke Monitoring

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

Local Area Network (LAN)

A Local Area Network (LAN) is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a Wide Area Network (WAN).

Logon

The identification and authentication sequence that authorizes a user's access to a computer. Conversely, "logoff" is the sequence that terminates user access to the system.

Major Application

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Malicious Code

Malicious code refers to programs that are written intentionally to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses, computer viruses, and worms.

Management Controls

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Mandatory Requirements

Those contractual conditions and technical specifications that are established by the Government as being essential to meeting required needs.

Master System Security Plan

A Master, or "umbrella," system security plan (SSP) is a document which provides an overall picture of the security of the systems under an Agency Associate Administrator's responsibility (or equivalent per NITR-4) and is a key component of the certification and accreditation process. Master SSPs are to be supported by subordinate system security plans for individual systems. The difference between a master and a subordinate SSP is that the master primarily provides direction for the security of the subordinate systems that are included under it. Certification testing of security controls is to be done at the subordinate SSP level.

Media

Any and all materials in which data and/or information may be stored and may include floppy disks, CD-ROMS, hard drives, software manuals, and papers.

Memorandum of Understanding/ Agreement (MOU/A)

A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

Mission Essential Infrastructure (MEI)

Critical infrastructures, physical, Cyber-based systems, or a combination, whose diminished capabilities would significantly impact the Federal Government's ability to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services; and the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. (Reference Presidential Decision Directive (PDD) 63, May 22, 1998.)

Mobile Code

Mobile code refers to programs (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. The term also applies to situations involving a large homogeneous collection of platforms (e.g., Microsoft Windows).

Monitoring

An ongoing activity that checks on the system, its users, or the environment.

Multiple Component Incident

A single incident that encompasses two or more incidents.

National Security Information

Information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

Network

An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking...) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, commerce services provider, or relying party).

Network Address Translation

An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box, located where the LAN meets the Internet, makes all necessary IP address translations. NAT serves three main purposes: (1) provides a type of firewall by hiding internal IP addresses; (2) enables a company to use more internal IP addresses (both are used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations); and (3) allows a company to combine multiple ISDN connections into a single Internet connection.

Network Administrator

A person who manages a local area network (LAN) within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

Networks

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Non-repudiation

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later legitimately deny having processed, stored, or transmitted the information.

OMB A-130, Appendix III

Establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

Operation/Mainte-nance

After initial system testing, the system is installed or fielded. Many security activities take place during the operational phase of a system's life. In general, these fall into three areas: (1) security operations and administration; (2) operational assurance; and (3) periodic re-analysis of the security.

Operational Controls

The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

Organization Computer Security Official

The designated Government person who is assigned the task of managing and maintaining the security of IT resources within a component.

Password

A string of characters used to authenticate an identity or to verify access authorization. [FIPS PUB 140-1]

Patch

A patch (sometimes called a "fix") is a "repair job" for a piece of programming. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and track the installation of patches.

Patch Management

The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.

Penetration Test

A planned attempt by authorized officials to circumvent security controls in order to identify security weaknesses that need to be corrected.

Personal Use

Activities conducted for purposes other than accomplishing official or otherwise authorized activity. Executive Branch employees are specifically prohibited from using IT resources to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using IT resources to support a personal private business also includes employees using IT resources to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of IT resources to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization (examples).

Plan of Action and Milestones

The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms are used to close security performance gaps, assist the Inspector General (IG) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities.

The POA&M presents the opportunity for an agency to highlight its progress and demonstrate improvements in the quality and security of its information security program. It is also designed to serve as a management tool specific to agency processes and as a point of comparison for OMB in its assessment of the overall maturity of the Federal Government's IT security status.

Though the POA&M is considered a comprehensive plan, OMB operates under the assumption that additional and more detailed project management plans exist for each corrective action item identified in the POA&M, and that additional sources (e.g., IG audit reports and risk assessments) are readily available to provide original documentation of each weakness. Thus, each POA&M element should be clearly traceable back to its original source(s).

Potential Impact

Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Privacy Act of 1974 (Pub. Law 93-579)

A law enacted by Congress to protect against an invasion of privacy through the misuse of records by Federal agencies which allows a citizen to learn how records are collected, maintained, used, and disseminated by the Federal Government. It also permits an individual to gain access to most personal information maintained by Federal agencies and to seek amendment of any incorrect or incomplete information.

Privileged Access

That which is granted to a user so that files, processes, and system commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.

Procedural Controls

Security measures that IT system managers impose through personnel actions rather than by electronic means. Also called administrative controls. Examples of procedural controls include using sign-in logs, documenting configuration changes, and filling out checklists.

Remote Logon

Accessing one system by way of another without having to log on to the destination host. For example, accessing System B by logging on to System A and linking directly from System A to System B without logging on a second time.

Request for Information (RFI)

An announcement requesting information from industry in regard to a planned acquisition and, in some cases, requesting corporate capability information.

Request for Proposal (RFP)

A formal solicitation document used in negotiated acquisitions normally exceeding $100,000 to communicate government requirements and to solicit proposals.

Request for Quotation (RFQ)

A less formal solicitation document used in negotiated acquisitions valued at $100,000 or less to communicate government requirements and to solicit quotations.

Residual Risk

The portion of risk remaining after the application of appropriate security controls in the information system.

Risk

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Risk Assessment

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

Risk Management

The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes: risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal approval to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

Risk Mitigation

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints.

Risk Reduction

The lessening of security exposure to an acceptable level. This requires the identification, analysis, selection, approval, and implementation of cost-effective IT security protective measures. Sometimes called "safeguard implementation."

Rules of Behavior

Rules of Behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.

Safeguards

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Scanning

Sending packets or requests to another system to gain information to be used in a subsequent attack.

Security

Security is a system property. Security is much more that a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms, which span the system both logically and physically.

Security Category

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Certification

A comprehensive evaluation of the management, operational, and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the remaining vulnerabilities in the information system after the implementation of such controls.

Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.

Security Impact Analysis

The analysis conducted by an agency official often during the continuous monitoring phase of the security certification and accreditation process to determine the extent to which changes to the information system have affected the security posture of the system.

Security Objectives

The five security objectives are integrity, availability, confidentiality, accountability, and assurance.

Security Plans

The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.

Security Policy

The statement of required protection of the information objects.

Security Requirements

Requirements levied on an information system derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

SAISO

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Sensitive Information

Sensitive Information refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

Sensitive But Unclassified

Information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes.

Sensitivity

Sensitivity in an information technology environment consists of the system, data, and applications which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

Serious Adverse Impact

An event causing temporary harm resulting in a negative effect on: mission or project schedules or cost; the confidentiality, integrity, and availability of "special management attention" or high or moderate impact systems; or the image and reputation of NASA. The consequence would be recoverable; but at a cost in tangible assets or resources (one million dollars or less), in customer or public confidence, and place NASA at a financial or technological disadvantage.

Significant Change

A modification, deletion, or addition to a system which may result in reducing the effectiveness of protective controls or in making additional protective controls necessary. Examples of significant changes include, but are not limited to, relocation to other facilities, major modification of the existing facilities, introduction of new equipment, addition or deletion of external interfaces, changes to system network connectivity, installation of new operating system software, patches to applications, new releases of software, installation of new application software, introduction of more sensitive data, or a substantial change to the system's risk posture that might affect others on the same network.

Social Engineering

The act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information that they do not realize will be used to attack a computer network.

Statement of Work

A statement of the technical specification in the RFP that describes the material, product, service, or system required by the Government.

Subordinate System Security Plan

A subordinate system security plan (SSP) is a document, which provides an overall picture of the security of the systems under a program, project, or system-owner's responsibility, and is a key component of the certification and accreditation process. Subordinate SSPs support the master SSP. The master SSP primarily provides direction for the security of the subordinate systems that are included under it. Certification testing of security controls are to be accomplished at the subordinate SSP level.

System

A system, as defined by this guideline, is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must: (1) be under the same direct management control; (2) have the same function or mission objective; (3) have essentially the same operating characteristics and security needs; and (4) reside in the same general operating environment.

System Administrator

A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A system administrator would perform systems programmer activities with regard to the operating system and other network control programs.

System Development Life Cycle (SDLC)

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System Interconnection

The direct connection of two or more IT systems for sharing data and other information resources.

System Operational Status

System Operational Status is either (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition

System Security Plan

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

TCP/IP

Transmission Control Protocol/Internet Protocol is the protocol suite used by the Internet. A protocol suite is the set of message types, their formats, and the rules that control how messages are processed by computers on the network.

Technical Controls

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Telecommunications

The term "telecommunications" means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Threat

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

Unauthorized Access

A person gains logical or physical access without permission to a network, system, application, data, or other resource.

Uniform Resource Locator URL

A Uniform Resource Locator is the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, the two URLs below point to two different files at the domain nist.gov. The first specifies an executable file that should be fetched using the FTP protocol; the second specifies a Web page that should be fetched using the HTTP (Web) protocol: ftp://www.nist.gov/stuff.exe; http://www.nist.gov/index.html.

Update

An update (sometimes called a "patch") is a "repair" for a piece of software (application or operating system). During a piece of software's life, problems (called bugs) will almost invariably be found. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software vendor's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and keep track of the installation of patches.

User Account

Authority granted to an individual to access a system or software application. Typically granted by system administrators with the approval of the system's line manager. To access an account, a user needs to be authenticated, usually by providing a password.

User Authentication

A process by which a system receives validation of a user's identity.

Verification

The process used by an independent agent to confirm or establish by testing, evaluation, examination, investigation or competent evidence, the effectiveness of the security controls in an information system.

Virtual Private Network (VPN)

A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.

Virus

See Computer Virus.

Vulnerability

A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Wireless Local Area Network (WLAN)

A type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.